

Secure remote access to MikroTik routers

Gyenese László

MikroTik Trainer, Academy Trainer

MUM Budapest
2019.05.31.

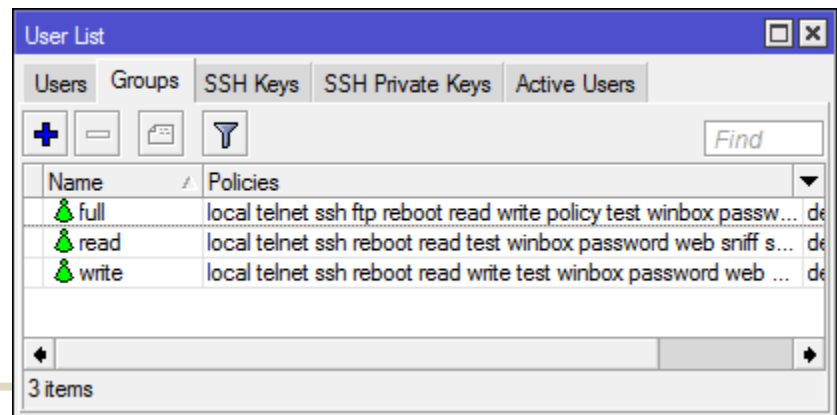
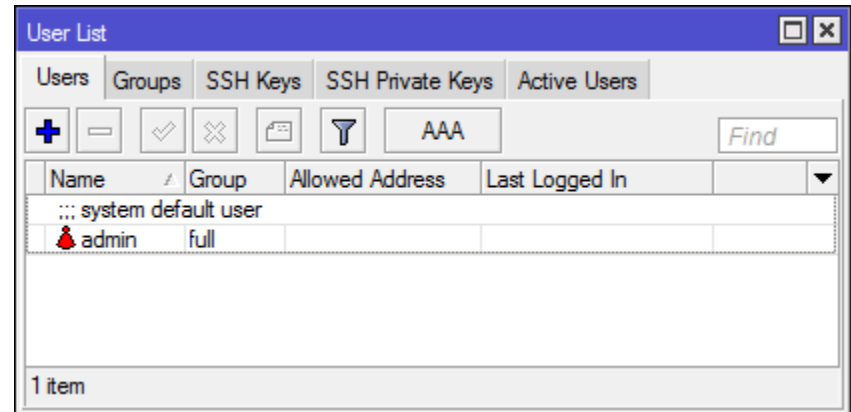
Protection against unauthorized access

Users

- Default password:
admin / <blank>

Change it!

- User groups with unique Policies



Protection against unauthorized access

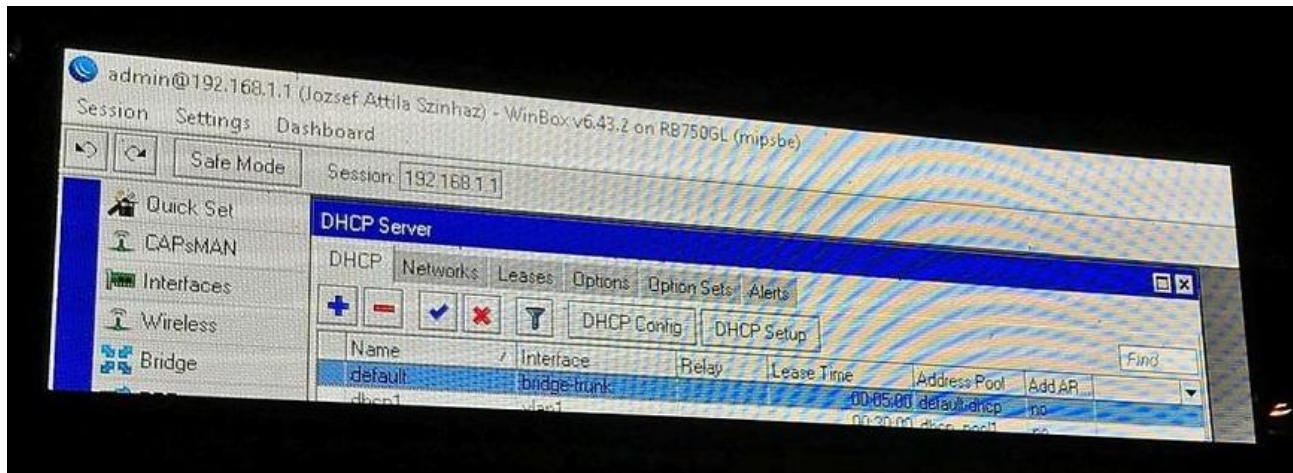
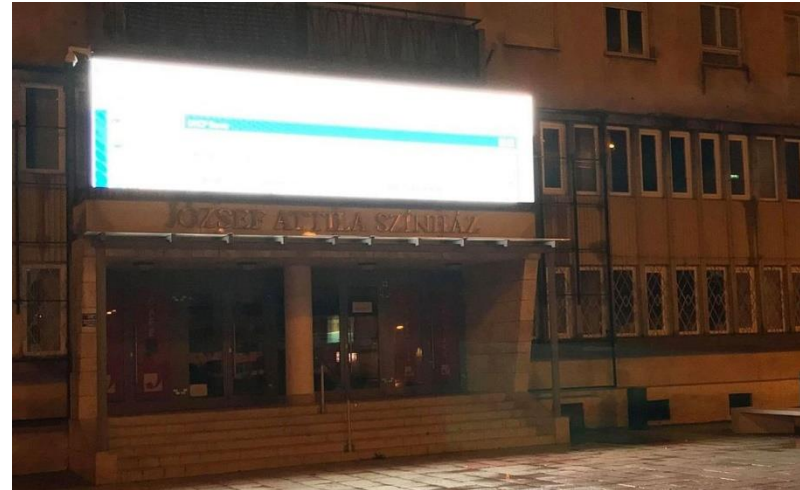
Login only from allowed addresses

The screenshot shows a window titled "User <KissPista>". It contains the following fields and controls:

- Name:** KissPista
- Group:** read (with a dropdown arrow)
- Allowed Address:** 192.168.1.0/24 (with a list box icon)
- Allowed Address:** 172.16.0.13 (with a list box icon)
- Last Logged In:** (empty text field)
- Buttons:** OK, Cancel, Apply (dashed border), Disable, Comment, Copy, Remove, Password...
- Status:** enabled (at the bottom left)

Protection against unauthorized access

Don't publish your settings



Protection against unauthorized access

Limiting services

	Name	Port	Available From	Certificate
X	api	8728		
X	api-ssl	8729		none
X	ftp	21		
X	ssh	22		
X	telnet	23		
	winbox	18291		
X	www	80		
X	www-ssl	443		none

8 items

IP Service <winbox>

Name: winbox

Port: 18291

Available From: 192.168.1.0/24

172.16.1.13

193.112.43.71

enabled

OK

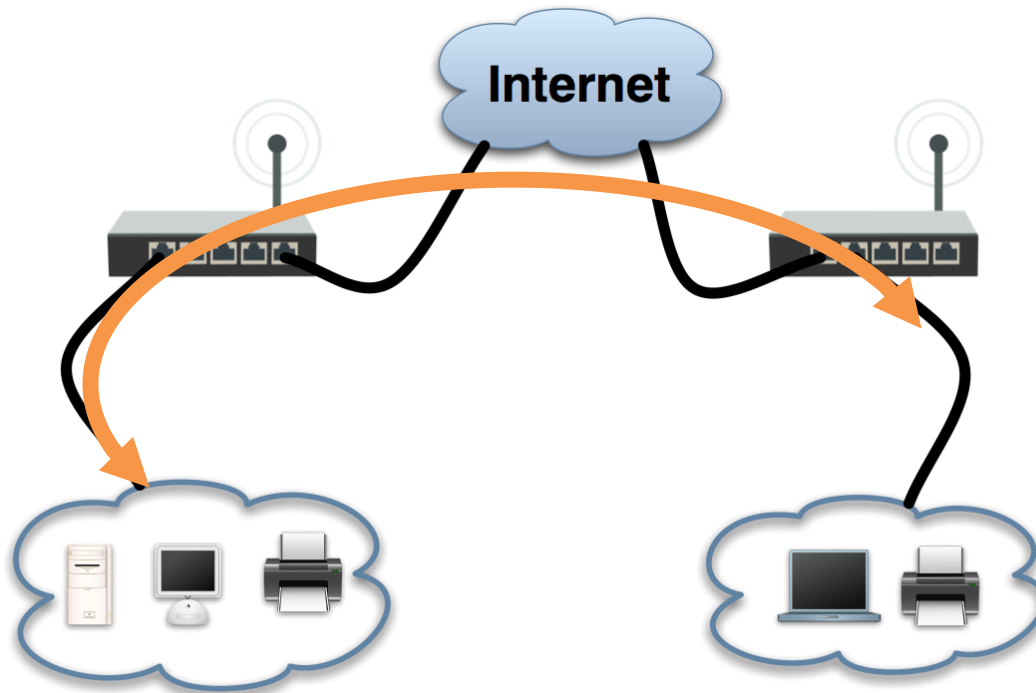
Cancel

Apply

Disable

Protection against unauthorized access

Secure access via VPN tunnel



Protection against unauthorized access

Access of services with „security code”:

1. You have to knock some ports on the router
2. In a short time you can access the router

Port Knocking

Port Knocking

You knock Router-ports in the correct order, e.g.:

1. 1 packet to UDP/10130 port
2. 2 packets to UDP/21516 port within 2 seconds
3. 1 packet to UDP/ 51123 port within 2 seconds

You have to create proper filter rules on the router!

If you knock in the proper code:

4. **Winbox login will enabled for 10 seconds**

Port Knocking – my own application

Functions:

- Winbox login with unique pre-saved parameters
- Centralized secure Router-database – even in the Cloud

You will see same router-list on your desktop PC, on your Laptop, etc. without manual synchronization of Winbox managed lists
- Unique Port Knocking configuration for all routers (if needed)

Port Knocking – my own application

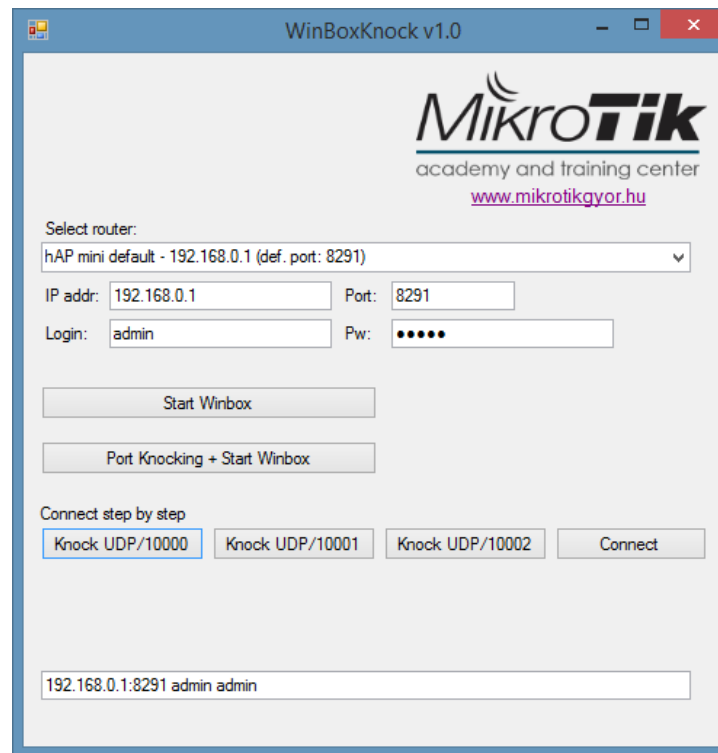
MikroTik router filter rules for port knocking example:

/ip firewall filter

```
add action=add-src-to-address-list address-list="Már tiltólistán vagy!" address-list-timeout=5s chain=input \
    dst-port=10000-10002 protocol=udp src-address-list=WinboxDenied
add action=add-src-to-address-list address-list=Knock1 address-list-timeout=10s chain=input dst-port=10000 \
    protocol=udp src-address-list=!WinboxDenied
add action=add-src-to-address-list address-list=Knock2 address-list-timeout=10s chain=input dst-port=10001 \
    protocol=udp src-address-list=Knock1
add action=add-src-to-address-list address-list=WinboxDenied address-list-timeout=20s chain=input dst-port=10001 \
    protocol=udp src-address-list=!Knock1
add action=add-src-to-address-list address-list=KnockOK address-list-timeout=10s chain=input dst-port=10002 \
    protocol=udp src-address-list=Knock2
add action=add-src-to-address-list address-list=WinboxDenied address-list-timeout=20s chain=input dst-port=10002 \
    protocol=udp src-address-list=!Knock2
add action=accept chain=input dst-port=8291 protocol=tcp src-address-list=KnockOK
```

Port Knocking – my own application

Let's see in practice...



The screenshot shows the WinBoxKnock v1.0 application window. It features the MikroTik logo and website URL at the top. Below, there's a 'Select router:' dropdown menu currently showing 'hAP mini default - 192.168.0.1 (def. port: 8291)'. To the right of the dropdown are input fields for 'IP addr:' (192.168.0.1) and 'Port:' (8291). Below these are 'Login:' (admin) and 'Pw:' (masked with dots) fields. There are two buttons: 'Start Winbox' and 'Port Knocking + Start Winbox'. A section titled 'Connect step by step' contains four buttons: 'Knock UDP/10000' (highlighted with a blue border), 'Knock UDP/10001', 'Knock UDP/10002', and 'Connect'. At the bottom, a text box displays the command '192.168.0.1:8291 admin admin'.

Most common router attacks

Including but not limited to:

- MNDP (CDP) attack
- DHCP attacks – Discovery, Rogue, ...
- TCP SYN attack
- UDP Flood
- Password Brute Force
- Port Scanner

MNDP (CDP) attack

Neighbor List

Discovery Settings

Find

Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Age (s)	Uptime	
 ether3-LAN		00:50:56:33:46:B6	01_Jose-...	Mikro Tik	6.42.5 (st...	x86	no	63	12:55:23	
 ether3-LAN		00:50:56:23:08:B2	01_Jose-...	Mikro Tik	6.42.5 (st...	x86	no	63	12:55:23	
 ether3-LAN		00:50:56				86	no	63	12:55:23	
 ether3-LAN		00:50:56				86	no	63	12:55:23	
 ether3-LAN		00:50:56				86	no	63	12:55:23	
 ether3-LAN		00:50:56				86	no	63	12:55:23	
 ether3-LAN		00:50:56				86	yes	43	00:40:19	
 ether3-LAN		00:50:56				86	yes	43	00:40:19	
 ether3-LAN		00:50:56				86	yes	43	00:40:19	
 ether3-LAN		00:50:56				86	yes	43	00:40:19	
 ether3-LAN		00:50:56:3A:F1:C7	ISP1	Mikro Tik	6.37.3 (st...	x86	yes	43	00:40:19	
 ether3-LAN		00:50:56:3C:8F:CB	ISP1	Mikro Tik	6.37.3 (st...	x86	yes	43	00:40:19	
 ether3-LAN		00:50:56:2D:E3:B4	ISP1	Mikro Tik	6.37.3 (st...	x86	yes	43	00:40:19	

Discovery Settings

Interface: NEIGHBOR

OK

Cancel

Apply

DHCP Starvation attacks

DHCP Server									
DHCP Networks Leases Options Option Sets Alerts + - ✓ ✗ 📄 🔍 Check Status Find									
	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address...	Active Host ...	Expires After	Status
D	192.168.1.2	3F:CC:BE:72:37:03		dhcp1	192.168.1.2	3F:CC:BE:72:37:03		00:00:06	offered
D	192.168.1.3	30:62:9D:3C:E3:82		dhcp1	192.168.1.3	30:62:9D:3C:E3:82		00:00:06	offered
D	192.168.1.4	6E:3A:1C:54:4E:75		dhcp1	192.168.1.4	6E:3A:1C:54:4E:75		00:00:06	offered
D	192.168.1.5	57:FB:9F:08:74:60		dhcp1	192.168.1.5	57:FB:9F:08:74:60		00:00:06	offered
D	192.168.1.6	EB:BE:49:7A:C3:49		dhcp1	192.168.1.6	EB:BE:49:7A:C3:49		00:00:06	offered
D	192.168.1.7	B0:3A:38:4E:A1:C9		dhcp1	192.168.1.7	B0:3A:38:4E:A1:C9		00:00:06	offered
D	192.168.1.8	6C:1E:E6:7C:33:1A		dhcp1	192.168.1.8	6C:1E:E6:7C:33:1A		00:00:06	offered
D	192.168.1.9	2B:63:CC:11:D1:41		dhcp1	192.168.1.9	2B:63:CC:11:D1:41		00:00:06	offered
D	192.168.1.10	8F:2C:AD:31:C6:9B		dhcp1	192.168.1.10	8F:2C:AD:31:C6:9B		00:00:06	offered
D	192.168.1.11	12:2F:8A:52:43:2B		dhcp1	192.168.1.11	12:2F:8A:52:43:2B		00:00:06	offered
D	192.168.1.12	93:92:14:5F:32:D9		dhcp1	192.168.1.12	93:92:14:5F:32:D9		00:00:06	offered
D	192.168.1.13	82:20:28:44:60:30		dhcp1	192.168.1.13	82:20:28:44:60:30		00:00:06	offered
D	192.168.1.14	DB:0A:BF:07:C9:B3		dhcp1	192.168.1.14	DB:0A:BF:07:C9:B3		00:00:06	offered
D	192.168.1.15	43:16:B9:00:C3:91		dhcp1	192.168.1.15	43:16:B9:00:C3:91		00:00:06	offered
253 items									

TCP SYN attacks

Firewall									
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols									
Tracking Find									
	Src. Address	Dst. Address	Proto...	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes	
C	1.1.196.241:29889	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B	
C	1.1.213.148:31538	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B	
C	1.6.33.104:36289	192.168.1.1:80	6 (tcp)		00:00:02	syn sent	0 bps/0 bps	160 B/0 B	
C	1.6.132.187:64285	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B	
C	1.6.175.4:42697	192.168.1.1:80	6 (tcp)		00:00:04	syn sent	0 bps/0 bps	160 B/0 B	
C	1.8.165.191:9503	192.168.1.1:80	6 (tcp)		00:00:01	syn sent	0 bps/0 bps	160 B/0 B	
C	1.8.173.46:62682	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B	
C	1.8.244.152:36349	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B	
C	1.9.212.87:40970	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B	
C	1.10.67.244:57959	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B	
C	1.10.102.91:5321	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B	
C	1.13.67.211:9280	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B	
C	1.13.189.198:14185	192.168.1.1:80	6 (tcp)		00:00:01	syn sent	0 bps/0 bps	160 B/0 B	
C	1.16.48.178:25762	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B	
C	1.18.139.155:61426	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	0 bps/0 bps	160 B/0 B	
C	1.19.155.158:13113	192.168.1.1:80	6 (tcp)		00:00:03	syn sent	0 bps/0 bps	160 B/0 B	
C	1.19.209.175:32379	192.168.1.1:80	6 (tcp)		00:00:03	syn sent	0 bps/0 bps	160 B/0 B	
C	1.21.42.131:47210	192.168.1.1:80	6 (tcp)		00:00:01	syn sent	0 bps/0 bps	160 B/0 B	
48601 items out of 300864				Max Entries: 1048576					

UDP Flood attacks

Firewall									
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols									
Tracking Find									
	Src. Address	Dst. Address	Protocol	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes	
C	1.1.124.145:16274	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B	▼
C	1.1.152.193:4070	192.168.1.1:53	17 (udp)		00:00:09		0 bps/0 bps	28 B/0 B	▲
C	1.1.210.234:39613	192.168.1.1:53	17 (udp)		00:00:03		0 bps/0 bps	28 B/0 B	
C	1.1.232.251:7299	192.168.1.1:53	17 (udp)		00:00:07		0 bps/0 bps	28 B/0 B	
C	1.2.43.209:20491	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B	
C	1.2.63.154:53419	192.168.1.1:53	17 (udp)		00:00:01		0 bps/0 bps	28 B/0 B	
C	1.2.124.175:15303	192.168.1.1:53	17 (udp)		00:00:01		0 bps/0 bps	28 B/0 B	
C	1.2.124.227:24114	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B	
C	1.2.166.33:39602	192.168.1.1:53	17 (udp)		00:00:00		0 bps/0 bps	28 B/0 B	
C	1.2.170.109:56965	192.168.1.1:53	17 (udp)		00:00:03		0 bps/0 bps	28 B/0 B	
C	1.2.201.185:55335	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B	
C	1.2.243.99:16763	192.168.1.1:53	17 (udp)		00:00:01		0 bps/0 bps	28 B/0 B	
C	1.2.252.77:55178	192.168.1.1:53	17 (udp)		00:00:08		0 bps/0 bps	28 B/0 B	
C	1.2.252.134:42559	192.168.1.1:53	17 (udp)		00:00:03		0 bps/0 bps	28 B/0 B	
C	1.3.179.240:49331	192.168.1.1:53	17 (udp)		00:00:00		0 bps/0 bps	28 B/0 B	
C	1.4.3.78:28758	192.168.1.1:53	17 (udp)		00:00:01		0 bps/0 bps	28 B/0 B	
C	1.4.15.108:36180	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B	
C	1.4.35.49:12614	192.168.1.1:53	17 (udp)		00:00:08		0 bps/0 bps	28 B/0 B	▼
177065 items out of 335494				Max Entries: 1048576					

Password Brute Force attacks

Torch (Running)

Basic

Interface: ether2-LAN

Entry Timeout: 00:00:03 s

Collect

☒ Src. Address ☒ Src. Address6

☒ Dst. Address ☒ Dst. Address6

☐ MAC Protocol ☒ Port

☒ Protocol ☐ VLAN Id

☐ 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

Start

Torch (Running)

Basic

Interface: ether2-LAN

Entry Timeout: 00:00:03 s

Collect

☒ Src. Address ☒ Src. Address6

☒ Dst. Address ☒ Dst. Address6

☐ MAC Protocol ☒ Port

☒ Protocol ☐ VLAN Id

☐ 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

Start

Stop

Close

New Window

Et...	Protocol	Src.	Dst.	Tx Rate
800 (ip)	6 (tcp)	192.168.1.254:39202	192.168.1.1:22 (ssh)	0 b/s
800 (ip)	6 (tcp)	192.168.1.254:45605	192.168.1.1:22 (ssh)	0 b/s
800 (ip)	6 (tcp)	192.168.1.254:38707	192.168.1.1:22 (ssh)	0 b/s
800 (ip)	6 (tcp)	192.168.1.254:40363	192.168.1.1:22 (ssh)	0 b/s
800 (ip)	6 (tcp)	192.168.1.254:57012	192.168.1.1:22 (ssh)	0 b/s
800 (ip)	6 (tcp)	192.168.1.254:51584	192.168.1.1:22 (ssh)	0 b/s
800 (ip)	6 (tcp)	192.168.1.254:40917	192.168.1.1:22 (ssh)	0 b/s
800 (ip)	6 (tcp)	192.168.1.254:59630	192.168.1.1:22 (ssh)	0 b/s
800 (ip)	6 (tcp)	192.168.1.254:42983	192.168.1.1:22 (ssh)	0 b/s
800 (ip)	6 (tcp)	192.168.1.254:56839	192.168.1.1:22 (ssh)	0 b/s
800 (ip)	6 (tcp)	192.168.1.254:42752	192.168.1.1:22 (ssh)	0 b/s
800 (ip)	6 (tcp)	192.168.1.254:58035	192.168.1.1:22 (ssh)	0 b/s
800 (ip)	6 (tcp)	192.168.1.254:34975	192.168.1.1:22 (ssh)	0 b/s
800 (ip)	6 (tcp)	192.168.1.254:52383	192.168.1.1:22 (ssh)	0 b/s
800 (ip)	6 (tcp)	192.168.1.254:57142	192.168.1.1:22 (ssh)	0 b/s
70 items	Total Tx: 0 bps	Total Rx: 0 bps	Total Tx Packet: 0	

Et...	Protocol	Src.	Dst.	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	6 (tcp)	192.168.1.254:40876	192.168.1.1:23 (telnet)	592 bps	1120 bps	1	2
800 (ip)	6 (tcp)	192.168.1.254:57657	192.168.1.1:23 (telnet)	968 bps	1056 bps	1	2
800 (ip)	6 (tcp)	192.168.1.254:44580	192.168.1.1:23 (telnet)	2.2 kbps	528 bps	1	1
800 (ip)	6 (tcp)	192.168.1.254:53595	192.168.1.1:23 (telnet)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:45764	192.168.1.1:23 (telnet)	0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.254:51001	192.168.1.1:23 (telnet)	0 bps	0 bps	0	0
6 items	Total Tx: 3.8 kbps	Total Rx: 2.7 kbps	Total Tx Packet: 3	Total Rx Packet: 5			

Port Scanner

 Zenmap

Scan Tools Profile Help

Target: 192.168.0.1 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.1

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

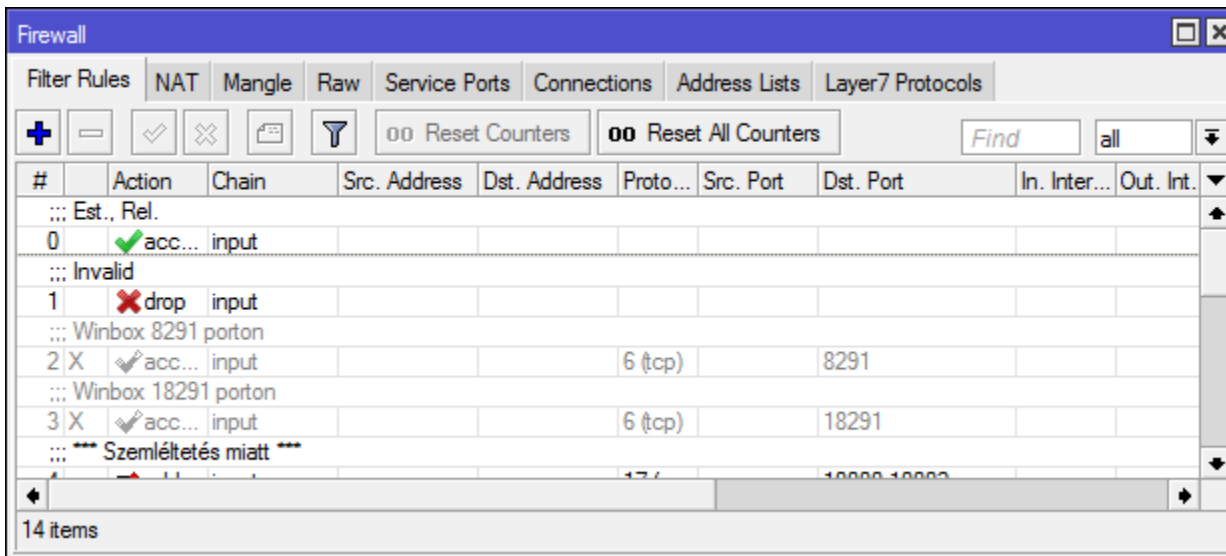
OS Host

```
nmap -T4 -A -v 192.168.0.1

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 11:44 Közép-európai nyári ido
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:44
Completed NSE at 11:44, 0.00s elapsed
Initiating NSE at 11:44
Completed NSE at 11:44, 0.00s elapsed
Initiating ARP Ping Scan at 11:44
Scanning 192.168.0.1 [1 port]
Completed ARP Ping Scan at 11:44, 1.33s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:44
Completed Parallel DNS resolution of 1 host. at 11:44, 16.55s elapsed
Initiating SYN Stealth Scan at 11:44
Scanning 192.168.0.1 [1000 ports]
Discovered open port 80/tcp on 192.168.0.1
Discovered open port 23/tcp on 192.168.0.1
Discovered open port 1723/tcp on 192.168.0.1
Discovered open port 1900/tcp on 192.168.0.1
Completed SYN Stealth Scan at 11:44, 2.50s elapsed (1000 total ports)
Initiating Service scan at 11:44
```

Preventing attacks

- Sophisticated Firewall system of RouterOS



- Unique protection for all forms of attack

Preventing attacks

- Rate-limiting for each new TCP connection
- Rate-limiting for each new UDP connection
- Disable DNS proxy on MikroTik if not required
- Limiting the number of times a user can unsuccessfully attempt to log in
- Users have to create and periodically change complex passwords
- Disabling unused services
- Port scanner limitations

Protect your routers!

How can you learn MikroTik security?



MikroTik Certified Security Engineer

a brand new MikroTik course since march 2019

Protect your routers!

First MikroTik Certified Security Engineers in Hungary



Győr



Budapest

Thank You!