Secure remote access to MikroTik routers

Gyenese László
MikroTik Trainer, Academy Trainer

MUM Budapest
2019.05.31.

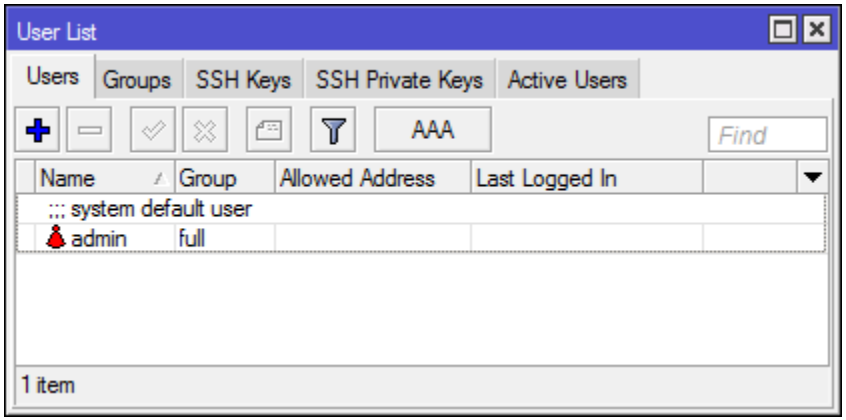
Protection against unauthorized access

Users

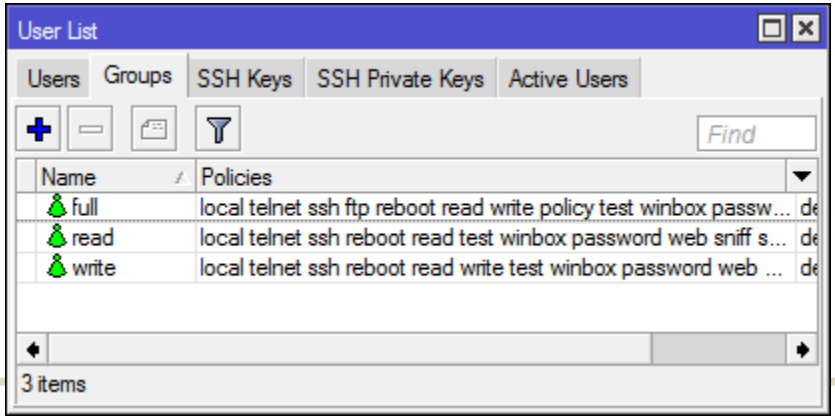
- Default password:

  admin / <blank>

  Change it!

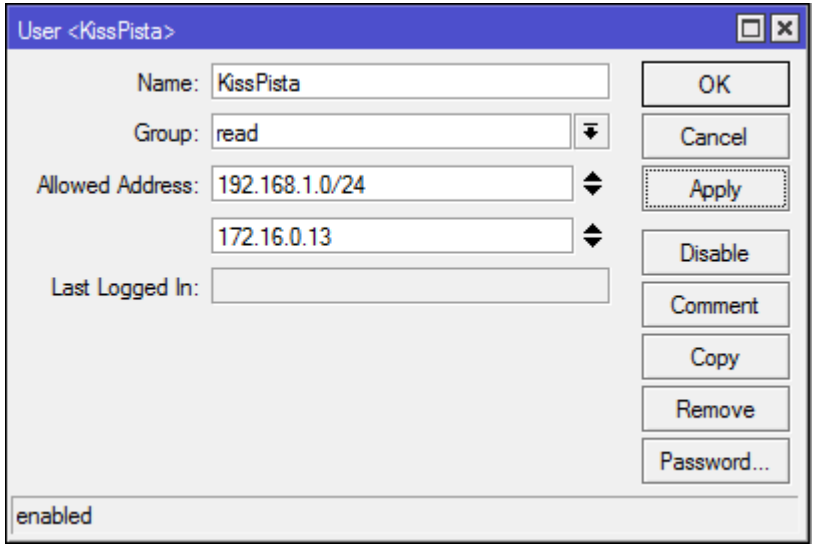


- User groups with unique Policies



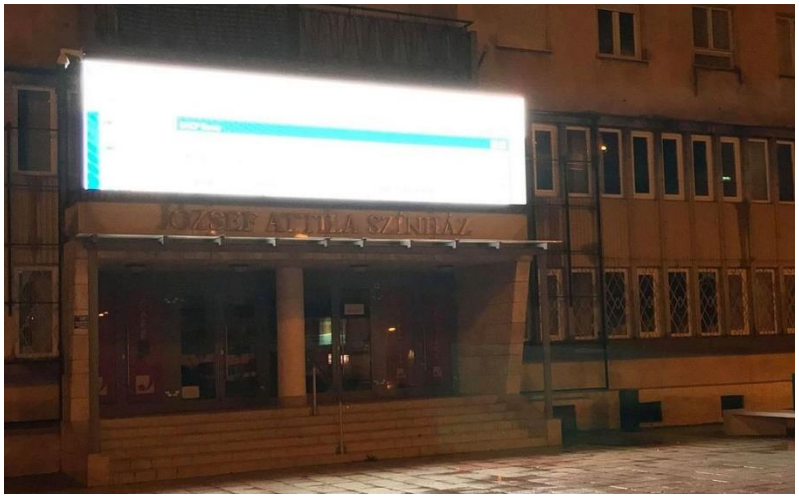
Protection against unauthorized access

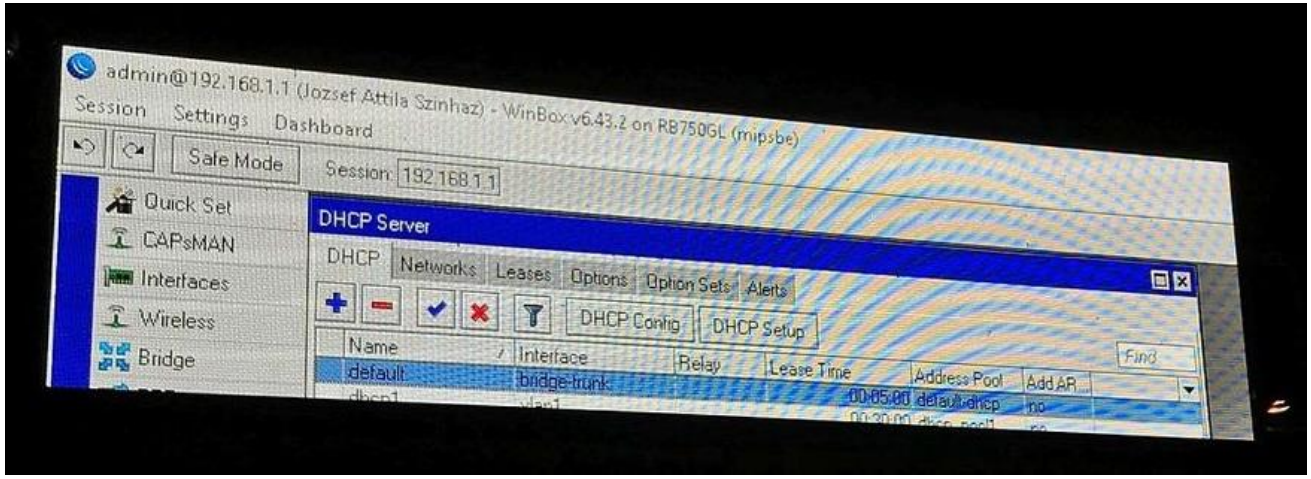
Login only from allowed addresses



Protection against unauthorized access

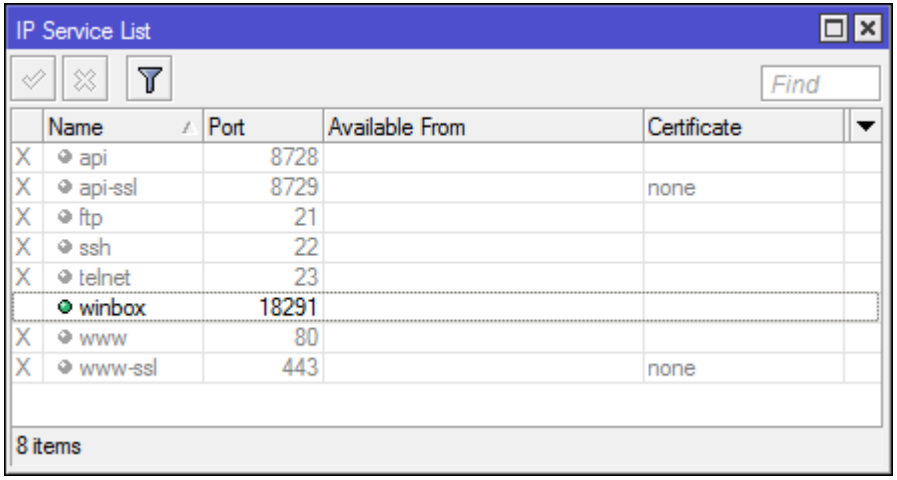
Don’t publish your settings

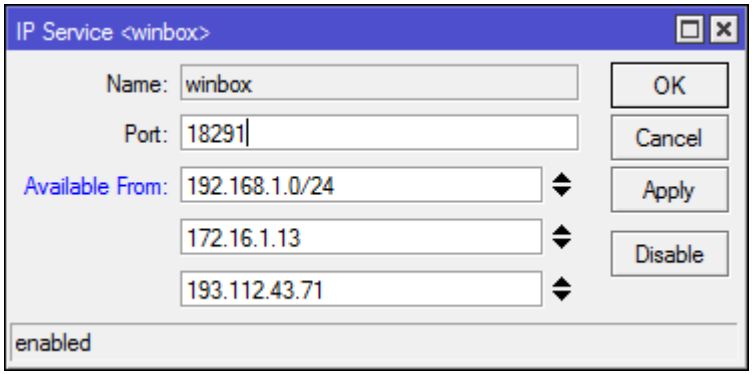




Protection against unauthorized access

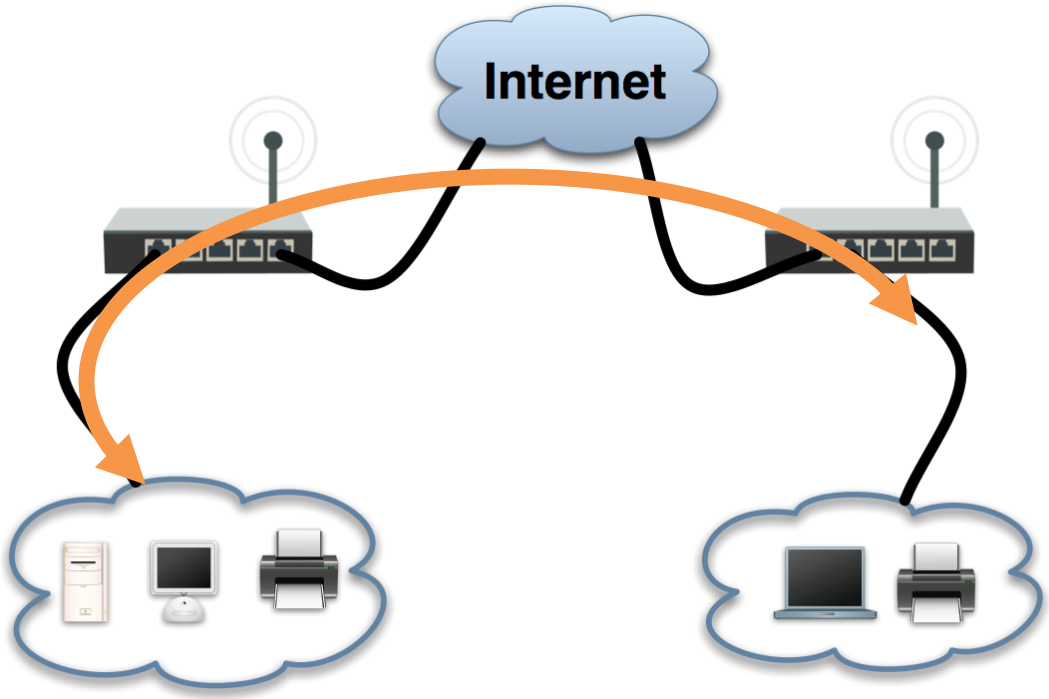
Limiting services





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)

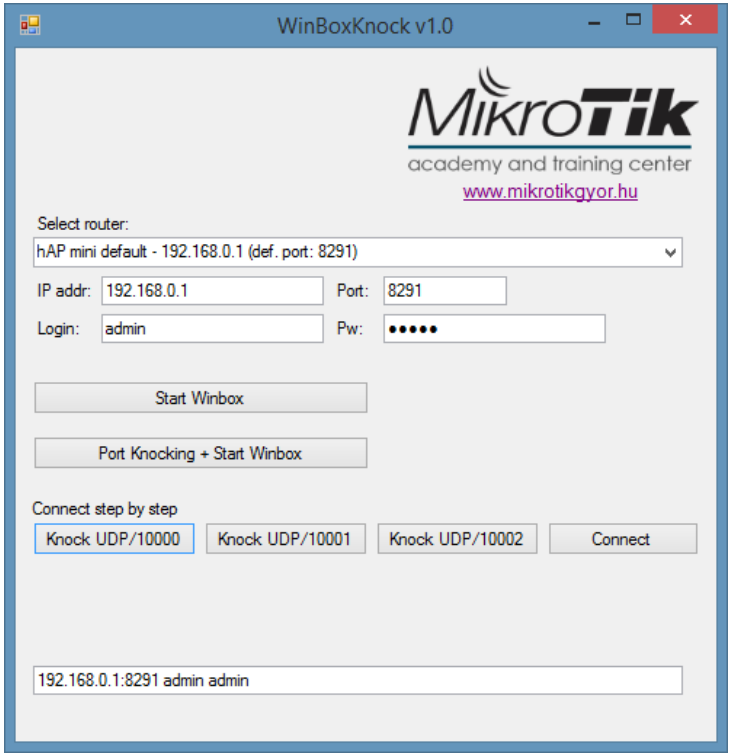
Port Knocking – my own application

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...

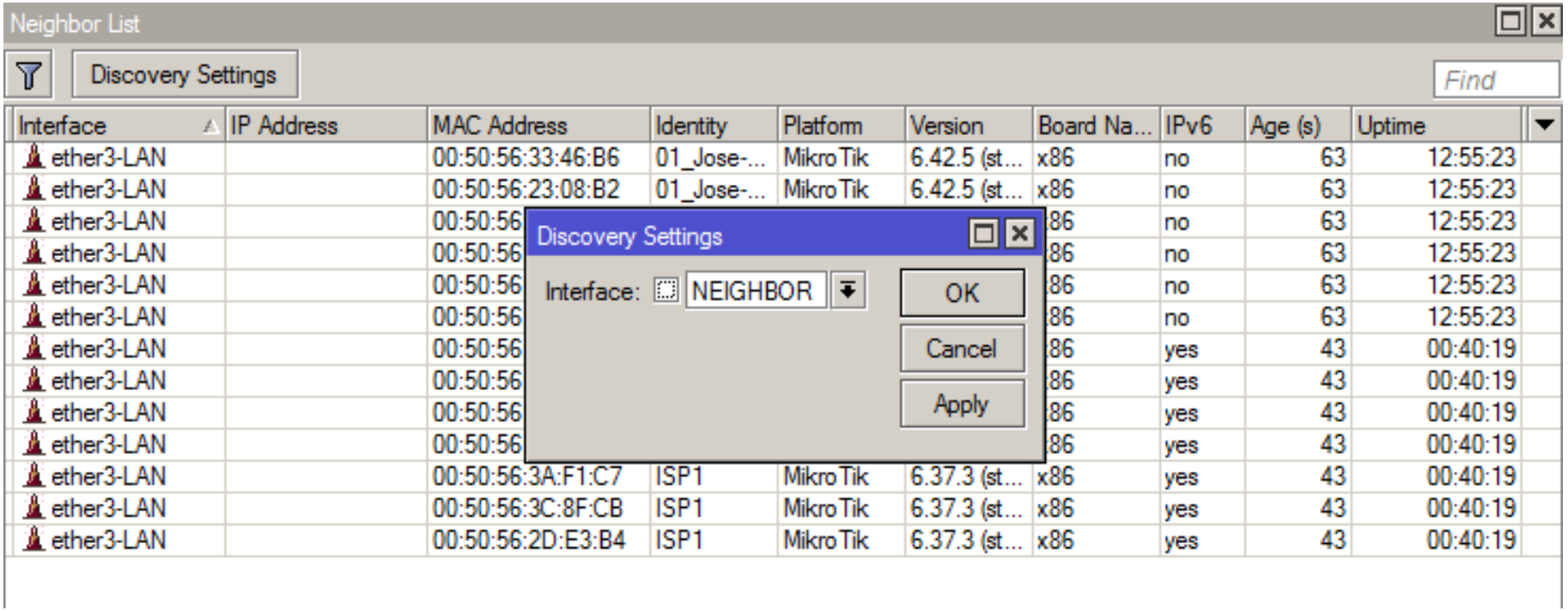


Most common router attacks

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



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 Addre...	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

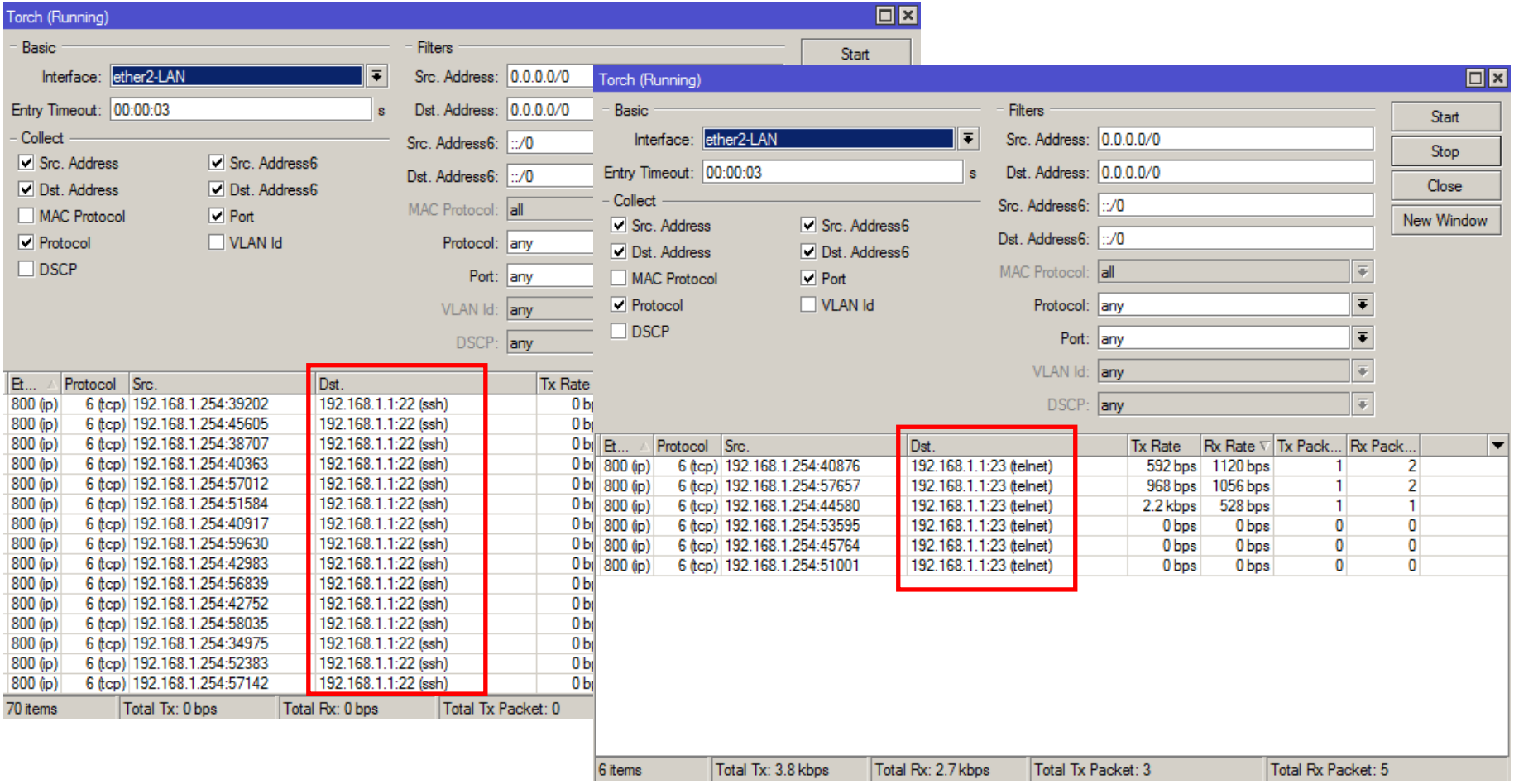
Tracking

Find

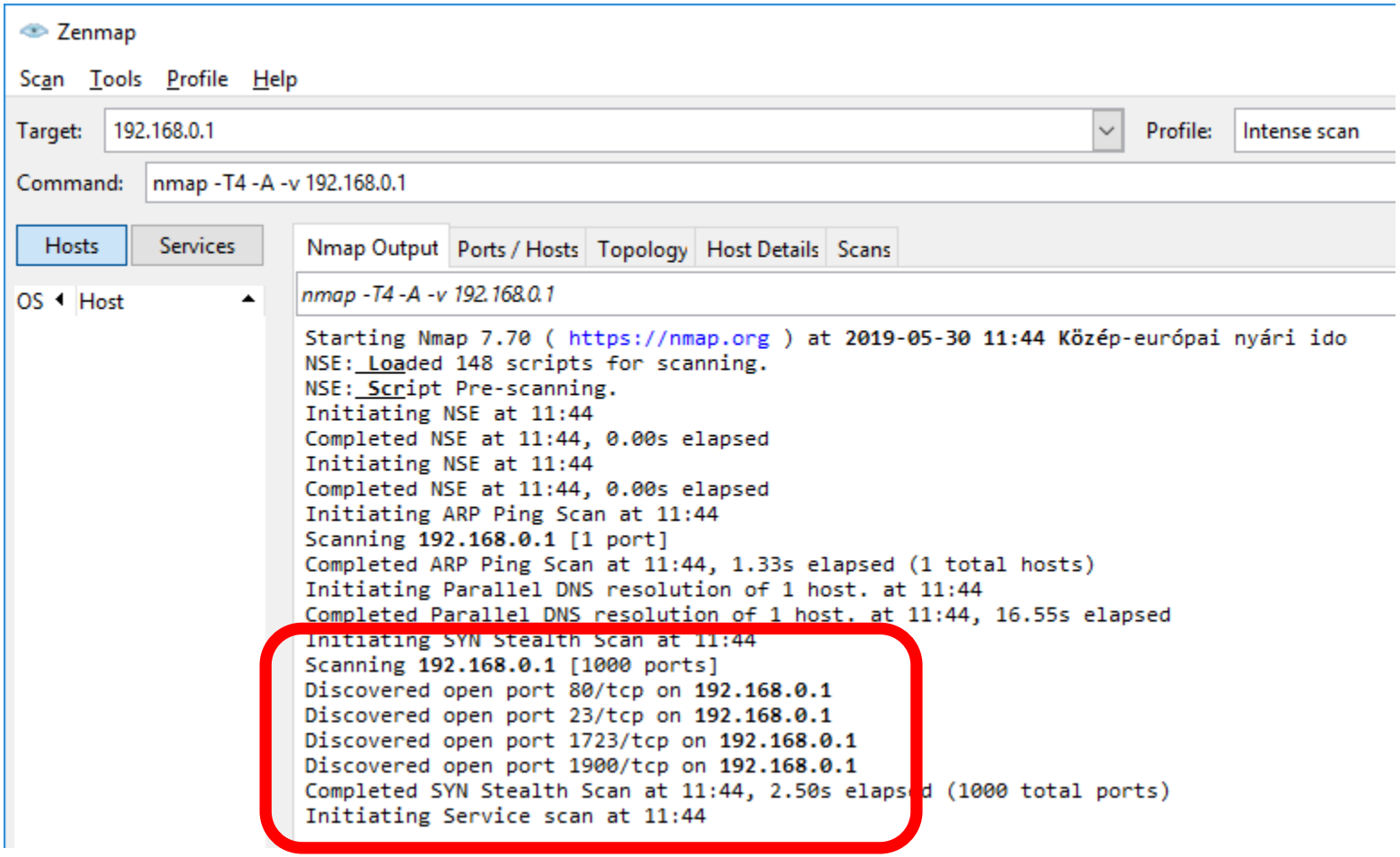
	Src. Address	Dst. Address	Protocol	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C	1.1.124.145:16274	192.168.1.1:53	17 (udp)		00:00:02		0 bps/0 bps	28 B/0 B
C	1.1.152.193:4070	192.168.1.1:53	17 (udp)		00:00:09		0 bps/0 bps	28 B/0 B
C	1.1.210.234:39613	192.168.1.1:53	17 (udp)		00:00:03		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

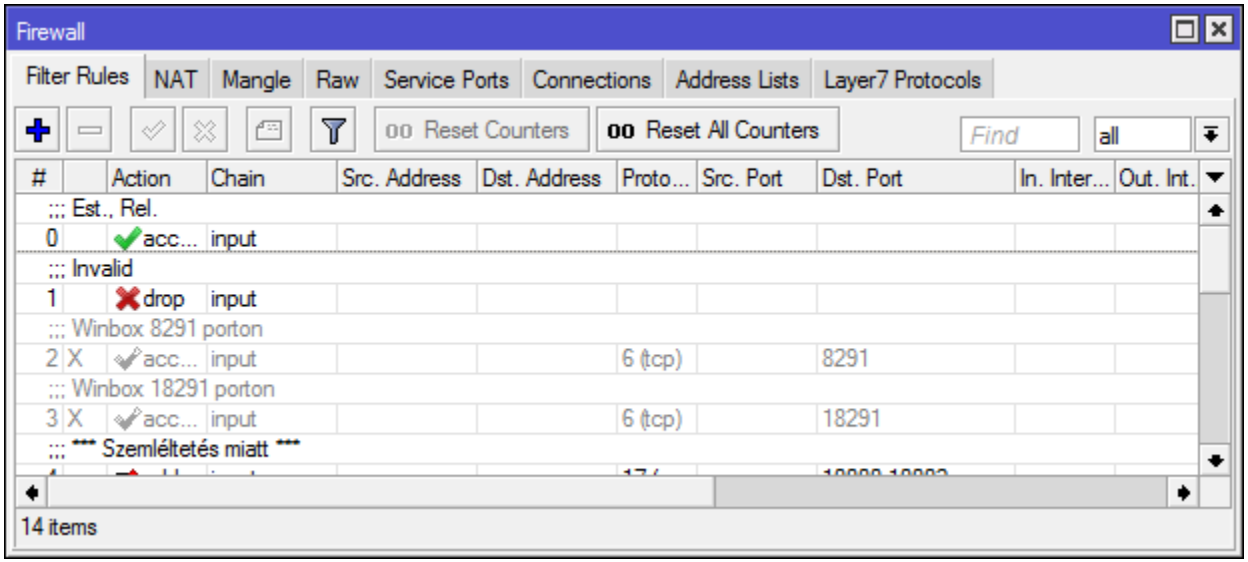


Port Scanner



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 reuired
- Limiting the number of times a user can unsuccessfully attemp 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!