

# RouterOS Güvenliđi

MUM İstanbul 2018

Osman Kazdal



Sekuritim Bilişim

**MikroTik**  
ROUTING THE WORLD



Ben Kimim?

Osman Kazdal

- MikroTik Certified Consultant
- MikroTik Certified Trainer
- CISSP
- Sekuritim Kurucusu

# Sekuritim Bilişim

- Value Added Master Distributor
- Eğitim Merkezi
- Danışmanlık
- Kurulum
- Destek
- 2008 yılında kurulmuştur.
- Ataşehir İstanbul





## İletişim

- Email: [info@sekuritim.com](mailto:info@sekuritim.com)
- Telefon: 0216 302 22 21
- Web: <https://sekuritim.com>
- Online satış: <https://shop.sekuritim.com>
- Facebook: <https://facebook.com/sekuritim>
- Twitter: <https://twitter.com/sekuritim>
- Reddit: <https://www.reddit.com/r/Sekuritim/>

# Training Center

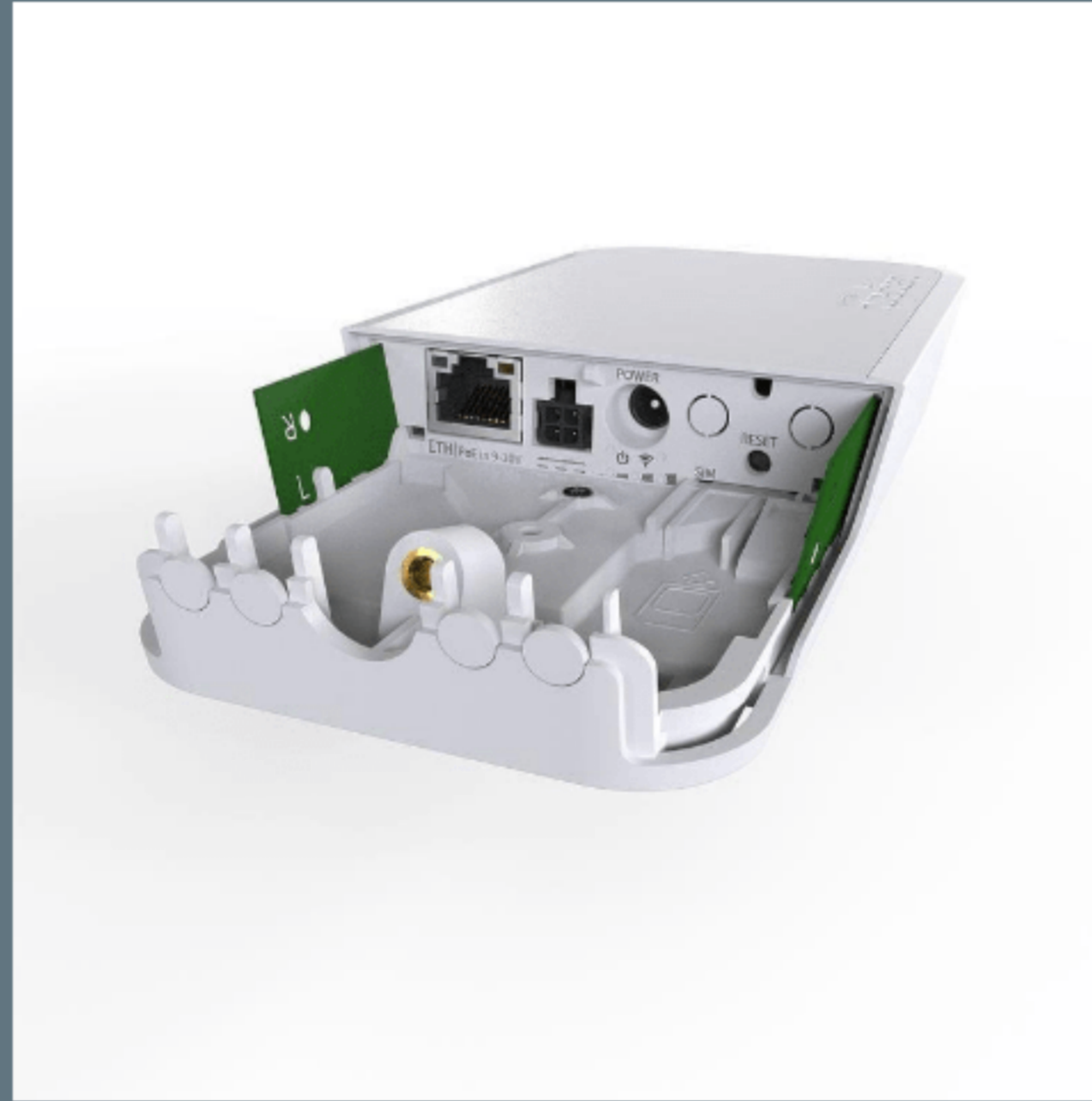
- Tüm MikroTik Sertifikasyon eğitimleri
- Türkiye'nin ilk MikroTik eğitmeni
- İstanbul merkezli, Türkiye'nin her yerinde
- Eğitim programı: <https://sekuritim.com/#trainings>
- Bilgi için: [training@sekuritim.com](mailto:training@sekuritim.com)



# Standımıza Bekliyoruz



# LTE Ürünleri

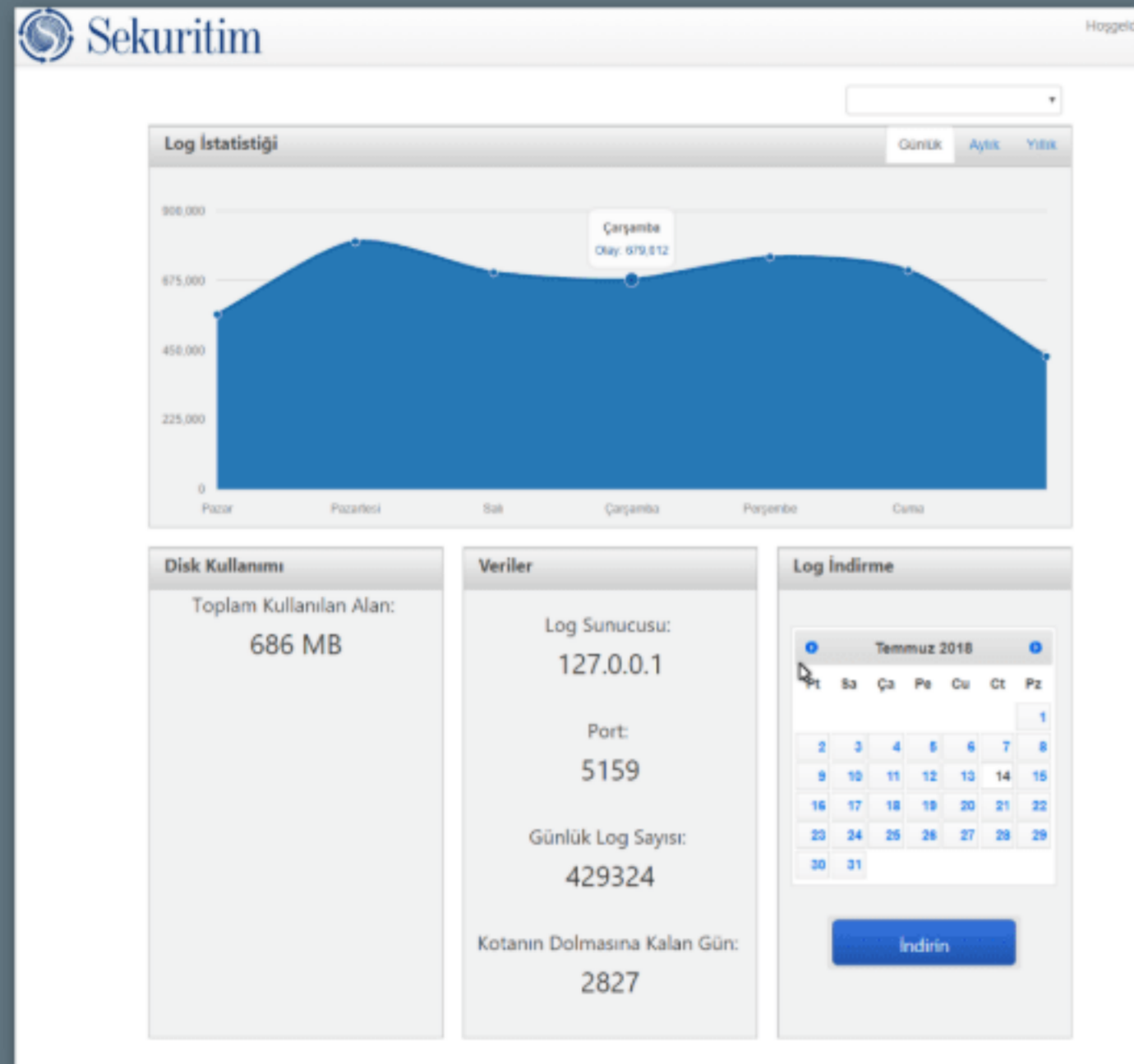


# Hotspot Çözümü





# 5651 Loglama Çözümü

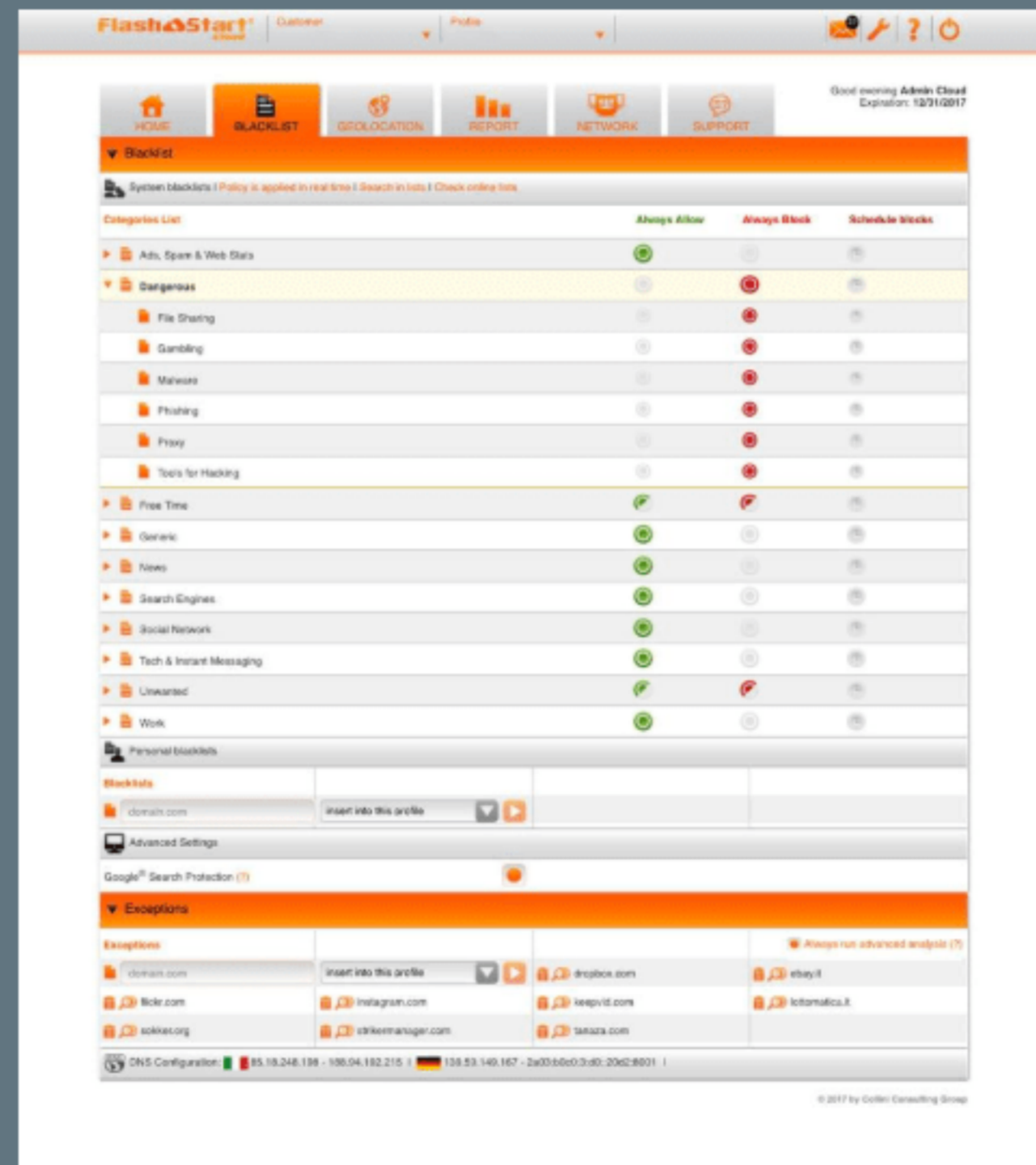


The screenshot shows a Windows desktop environment. In the foreground, a digital certificate window is open, titled 'Kamu Sertifikasyon Merkezi'. The certificate details include: 'Dosya Adı: [redacted].20170315.log', 'Açıklama: [redacted]', and 'Parnak Bil Değeri: TCL5vaxLnD4YpwN63DRB3nVfaQHasRz909CesTuzo='. The certificate is dated '16 March 2017 Thursday 01:00:02.633 GMT'. Below the certificate, there is a 'Zaman Damgası Bilgileri' section with a table of metadata.

Zaman Damgası Bilgileri			
Dosya:	E:\Users\paman\Downloads\20170315...20170315.log		
Damga Tarihi:	16.03.2017 04:00:02 EET +0300	Sen No:	001607966
Damağı Veren Makam:		Dosya Çeşit Tipi:	SHA-256
CH-Kamu SM Zaman Damgası Sunucusu Sunum 2		Zaman Damgasındaki Dosya Çeşit	
OU=SELGEM		TCL5vaxLnD4YpwN63DRB3nVfaQHasRz909CesTuzo=	
O=Ulkiye Bilimsel ve Teknolojik Arastirma Kurumu-TUBITAK		Şu Anki Dosya Çeşit	
L=Ölçer-Kocaeli		TCL5vaxLnD4YpwN63DRB3nVfaQHasRz909CesTuzo=	
C=TR		Dosya Değişmemiş	

The background shows a file explorer window with a list of files, including '20170315.log' (3 MB) and '20170315.log.txt' (2 KB). The desktop also shows icons for 'DUDE-1036...', 'OSPF-Main...', 'Avast Premier', and 'Zamane 2.0.5-SNAPSHOT'.

# FlashStart İçerik Filtreleme



# Referanslarımız

Sony Eurasia  
Turkcell Superonline  
Vodafone  
TEB Yatırım  
Panço Giyim  
Çayla Restoranları  
Çaytaş  
Esenyurt Üniversitesi  
MyFi  
Netspeed  
Telekom19





## RouterOS Güvenliđi

Nasıl saldırıyorlar?

Neden saldırıyorlar?

Kendimizi nasıl koruruz?



# Demo



## Saldırının Aşamaları

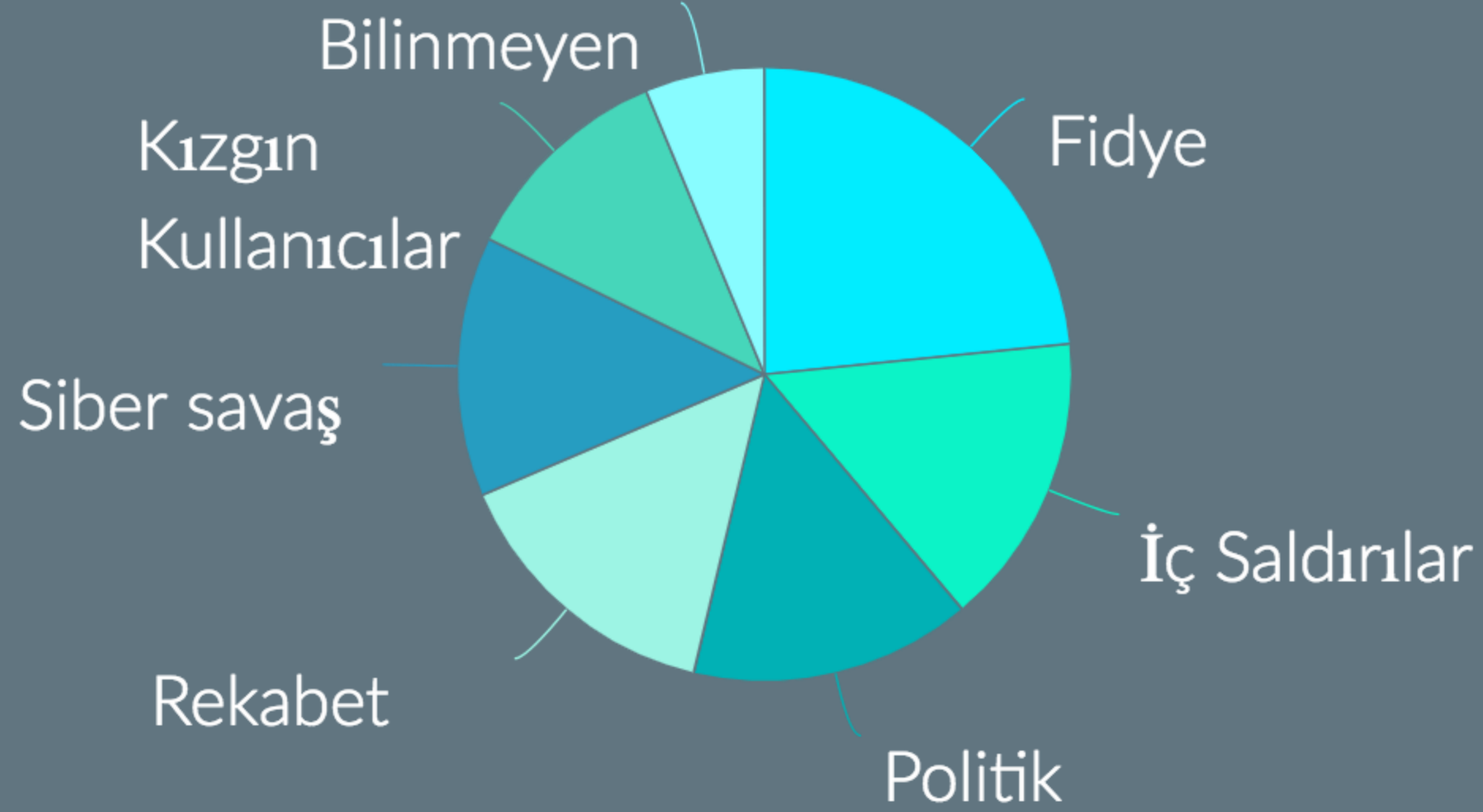
- Port tarama ile MikroTik router tespit edilmesi
- Winbox açığına kullanılarak şifrelerin ele geçirilmesi
- Router'ın ele geçirilmesi

# Ne yaptılar?

```
/ip firewall filter
add action=tarpit chain=input comment="Add you ip address to allow-ip in Address Lists." dst-port=30553 protocol=tcp
add action=add-src-to-address-list address-list=allow-ip address-list-timeout=1h chain=input comment="The security flaw for Hajime is closed by the firewall." packet-size=1083 protocol=icmp
add action=accept chain=input comment="Please update RotherOS and change password." src-address-list=allow-ip
add action=drop chain=input comment=" Thanks are accepted on WebMoney Z399578297824" dst-port=53 protocol=udp
add action=drop chain=input comment="or BTC 14qiYkk3nUgsdqQawiMLC1bUGDZWHowix1" dst-port=53,8728,8729,21,22,23,80,443,8291 protocol=tcp
add action=passthrough chain=input
/system note
set note="The security flaw for Hajime is closed by the firewall. Please update RotherOS. Gratitude is accepted on WebMoney Z399578297824 or BTC 14qiYkk3nUgsdqQawiMLC1bUGDZWHowix1"
```

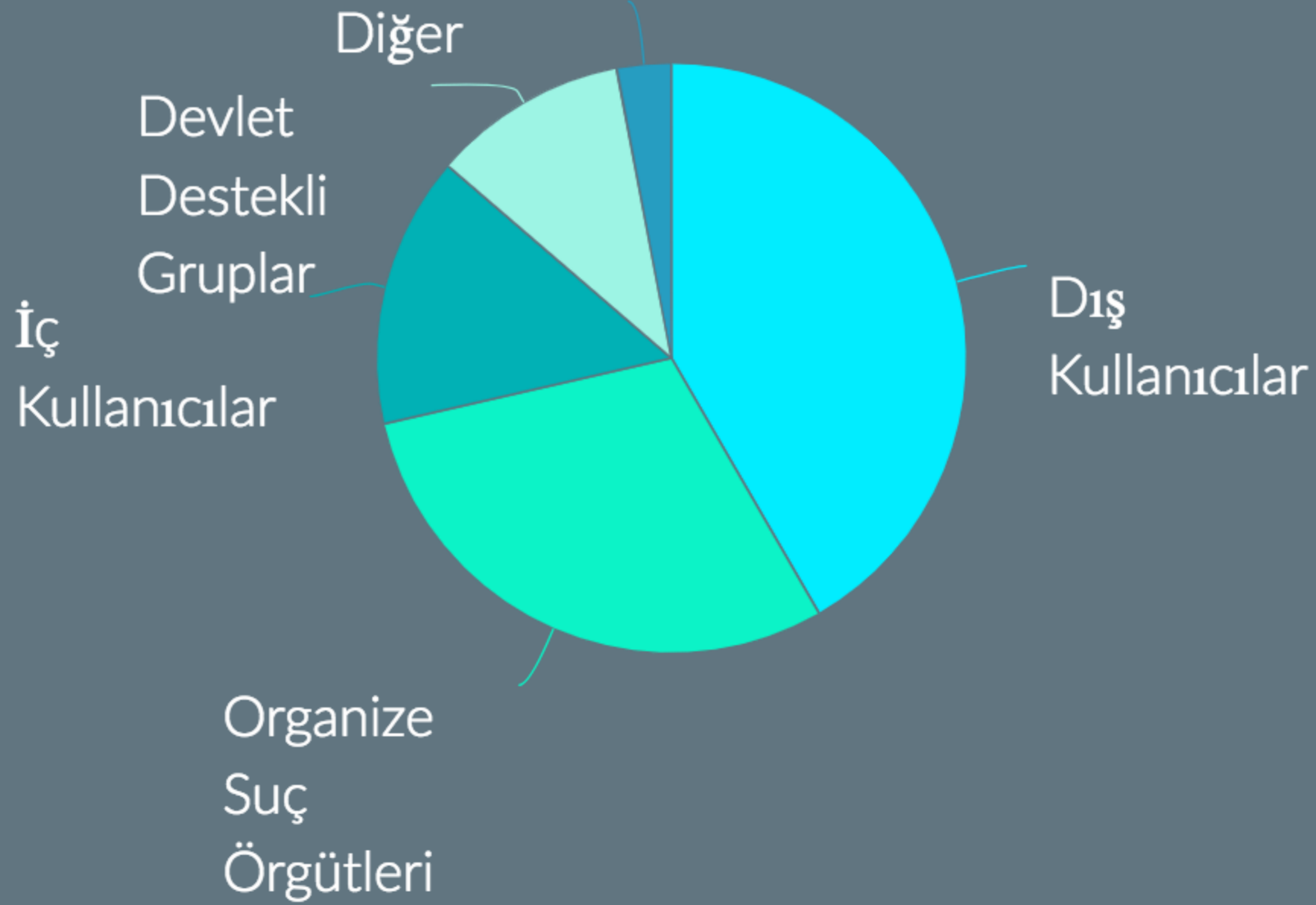
<https://forum.mikrotik.com/viewtopic.php?t=134804>

# Neden Saldırıyorlar?





# Kim Saldırıyor?

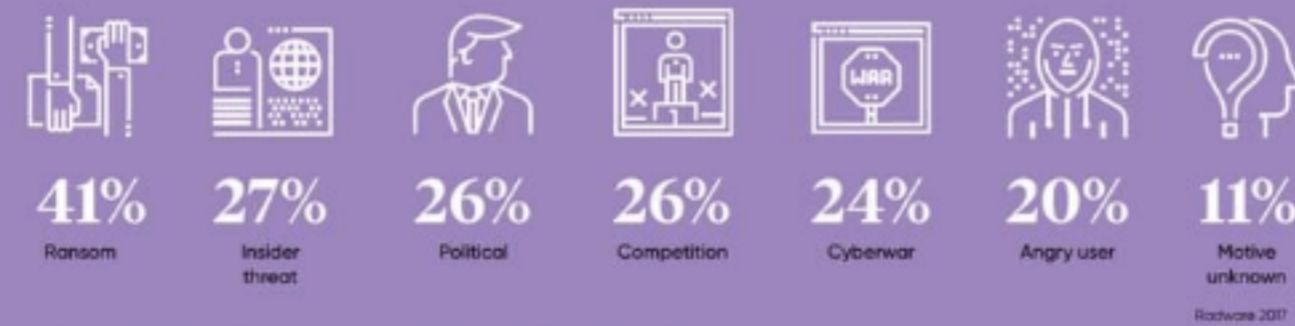


# Infograph

## WHY HACKERS HACK

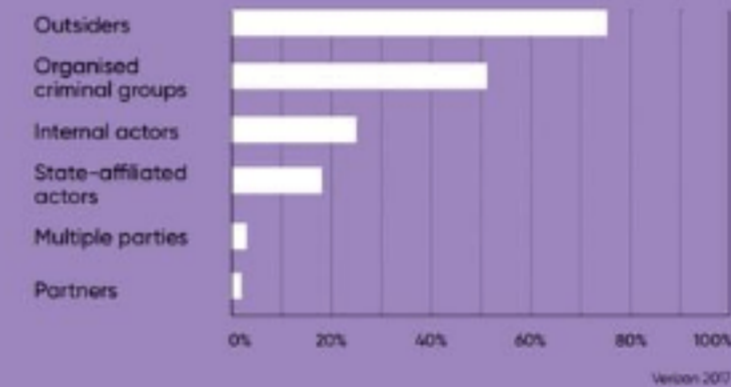
### MOTIVES BEHIND CYBERATTACKS

GLOBAL STUDY OF LARGE ORGANISATIONS THAT WERE VICTIMS TO A CYBERATTACK



### WHO'S BEHIND DATA BREACHES?

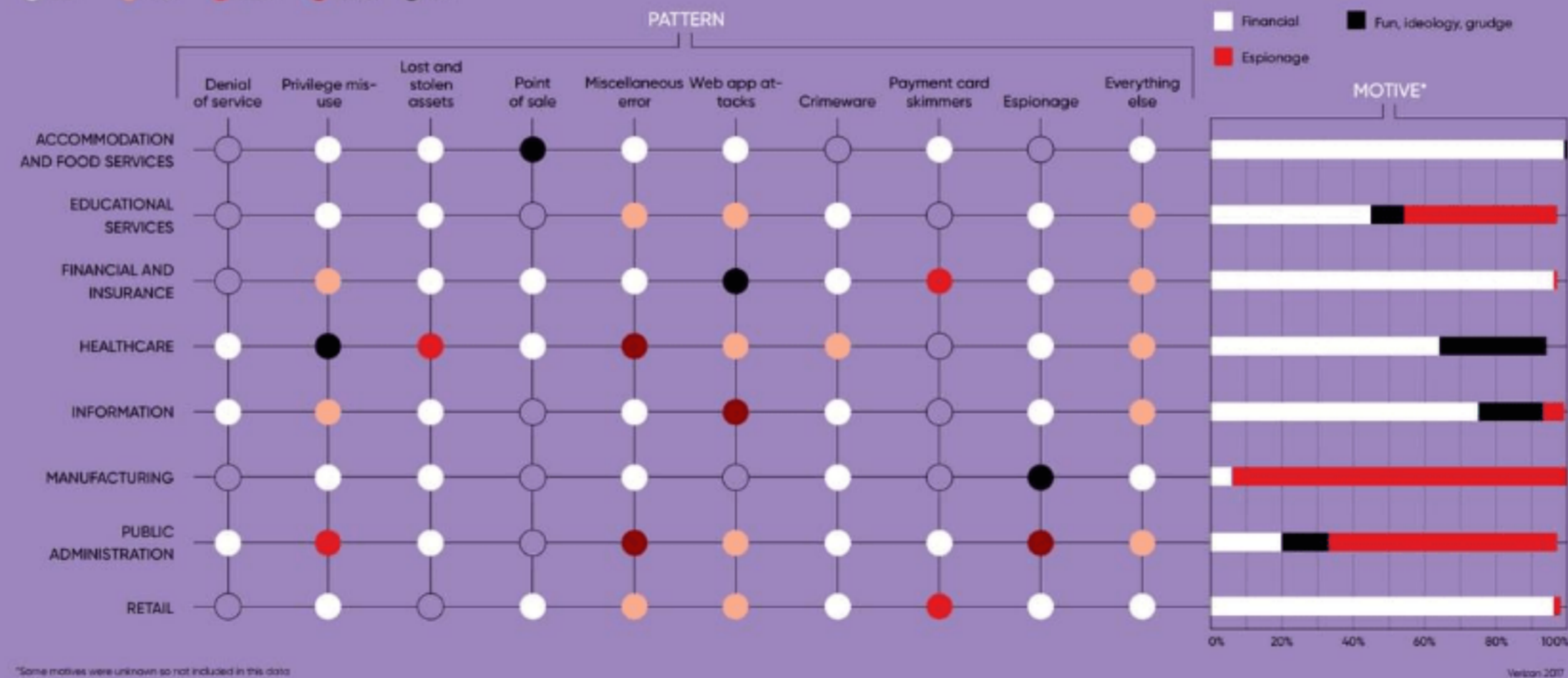
GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES



### DATA BREACHES, BY PATTERN AND MOTIVE

GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES

● 1-10 ● 11-30 ● 31-60 ● 61-100 ● 101+



RACONTEUR

<http://rcnt.eu/2mj57>

## Sık Görülen Saldırıları

- Portscanning
- Şifre Saldırıları - Brute force
- Uygulama Saldırıları - Winbox saldırısı
- Web Uygulama Saldırıları
- DoS & DDoS
- Zero Day saldırıları

# MikroTik Web Servis Açığı



The screenshot shows the WikiLeaks website interface. The main heading is "Vault 7: CIA Hacking Tools Revealed". To the right is the CIA logo. Below the heading, there are tabs for "Releases" and "Documents". A navigation breadcrumb trail reads: "Navigation: » Directory » Network Devices Branch (NDB) » Network Devices Branch » Operations/Testing » Perseus » Perseus 1.1.0". The document title is "DUT4 - RB1100AH - v1.1.0 Notes". Below the title, the following information is listed: "Owner: User #14587667", "IP: 172.20.100.22/30", "VLAN: 615 (TOR6 gi1/0/11)", and "ROS: 6.30.2, 6.26".

[https://wikileaks.org/ciav7p1/cms/page\\_28251293.html](https://wikileaks.org/ciav7p1/cms/page_28251293.html)

- <https://wikileaks.org/ciav7p1/>
- 7 Mart 2017'de yayınlandı.
- 9 Mart 2017'de MikroTik açığın giderildiği yeni sürümleri çıkardı.
- Etkilenmemek için güncel RouterOS kullanılmalı.
- İhtiyacınız yoksa www servisini kapatınız.

# MikroTik Web Servis Açığı

- VPNFilter
- Hajime Botnet
- Slingshot

Funny command

```
$ ./tools/getROSbin.py 6.38.4 mipsbe /nova/bin/www www_binary  
$ ./StackClash_mips.py 192.168.8.1 80 www_binary "echo hello world > /dev/lcd"
```



# MikroTik Winbox Açığı

## How to use

Note that this script will NOT run with Python2.x. Use only Python 3+

### Winbox (TCP/IP)

```
$ python3 WinboxExploit.py 172.17.17.17
```

```
User: admin  
Pass: Th3P4ssWord
```

### MAC server Winbox (Layer 2)

You can extract files even if the device doesn't have an IP address :-)

```
$ python3 MACServerDiscover.py  
Looking for Mikrotik devices (MAC servers)
```

```
aa:bb:cc:dd:ee:ff
```

```
aa:bb:cc:dd:ee:aa
```

```
$ python3 MACServerExploit.py aa:bb:cc:dd:ee:ff
```

```
User: admin  
Pass: Th3P4ssWord
```

- 23 Nisan 2018'de açığa çıktı.
- Aynı gün açığın giderildiği RouterOS sürümü yayınlandı.
- Uygulaması çok kolay olduğundan etkisi çok fazla.
- Güncel RouterOS sürümü kullanılmalı.
- Winbox erişimi filtelenmelidir

# Port Tarama

```
λ nmap -sS 192.168.1.1

Starting Nmap 7.31 ( https://nmap.org ) at 2018-10-11 22:23 Turkey Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.0038s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
443/tcp   open  https
2000/tcp  open  cisco-sccp
8080/tcp  open  http-proxy
8291/tcp  open  unknown
MAC Address: 98:9F:83:88:88:88 (Routerboard.com)

Nmap done: 1 IP address (1 host up) scanned in 14.25 seconds
```

- En çok kullanılan hedef tespit yöntemidir.
- MikroTik ürünler 80 ve 8291 portları taranarak bulundu.
- IP Firewall ve IP services ayarları ile engellenebilir

# Şifre Saldırıları

Oct/12/2018 23:38:32	memory	system, error, critical	login failure for user user from 103.89.89.228 via ssh
Oct/12/2018 23:38:32	memory	system, error, critical	login failure for user support from 103.89.89.228 via ssh
Oct/12/2018 23:38:32	memory	system, error, critical	login failure for user guest from 103.89.89.228 via ssh
Oct/12/2018 23:38:33	memory	system, error, critical	login failure for user root from 103.89.89.228 via ssh
Oct/12/2018 23:38:33	memory	system, error, critical	login failure for user user from 103.89.89.228 via ssh
Oct/12/2018 23:42:17	memory	certificate, info	got CRL with bad signature, issued by AddTrust External CA Root::SE:A
Oct/12/2018 23:42:17	memory	certificate, info	got CRL with bad signature, issued by GlobalSign Organization Validatio
Oct/13/2018 00:08:39	memory	system, error, critical	login failure for user root from 103.89.89.228 via ssh
Oct/13/2018 00:08:40	memory	system, error, critical	login failure for user user from 103.89.89.228 via ssh
Oct/13/2018 00:08:44	memory	system, error, critical	login failure for user support from 103.89.89.228 via ssh
Oct/13/2018 00:08:48	memory	system, error, critical	login failure for user user from 103.89.89.228 via ssh
Oct/13/2018 00:08:49	memory	system, error, critical	login failure for user guest from 103.89.89.228 via ssh

- Brute force şifre saldırıları
- Winbox açığı kullanıldığında şifre saldırıları yapmadan şifreler açığa çıktı.
- Şifre saldırılarına karşı karmaşık şifreler kullanılmalıdır
- IP Firewall ve IP services ayarlarından router'a bağlanabilecek IP adresleri kısıtlanmalıdır.

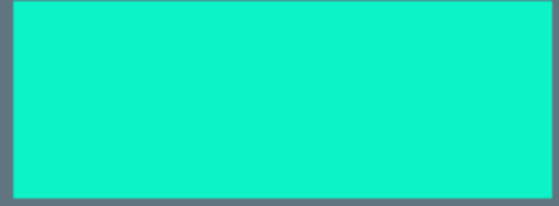




# DoS & DDoS Saldırıları

## Zero Day Saldırıları

- Bu yıl ve 2019 yılında saldırıların devam etmesi bekleniyor.
- 2017 Mart ayından beri artık MikroTik ürünler tüm hacker gruplarının hedefleri arasına girmiş durumda.
- Yeni açıklar her an çıkabilir.



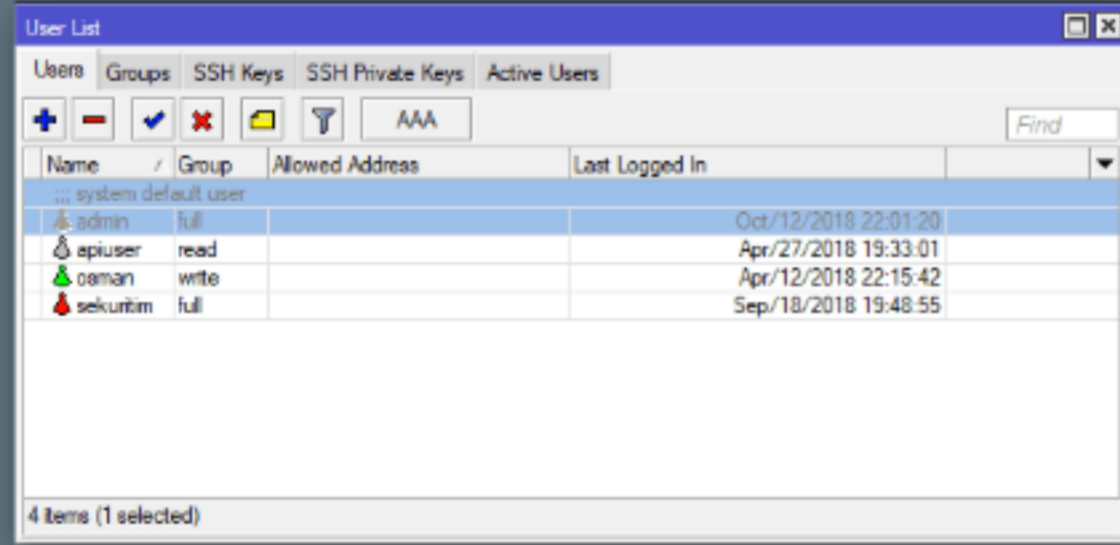
Ne Yapacađız?



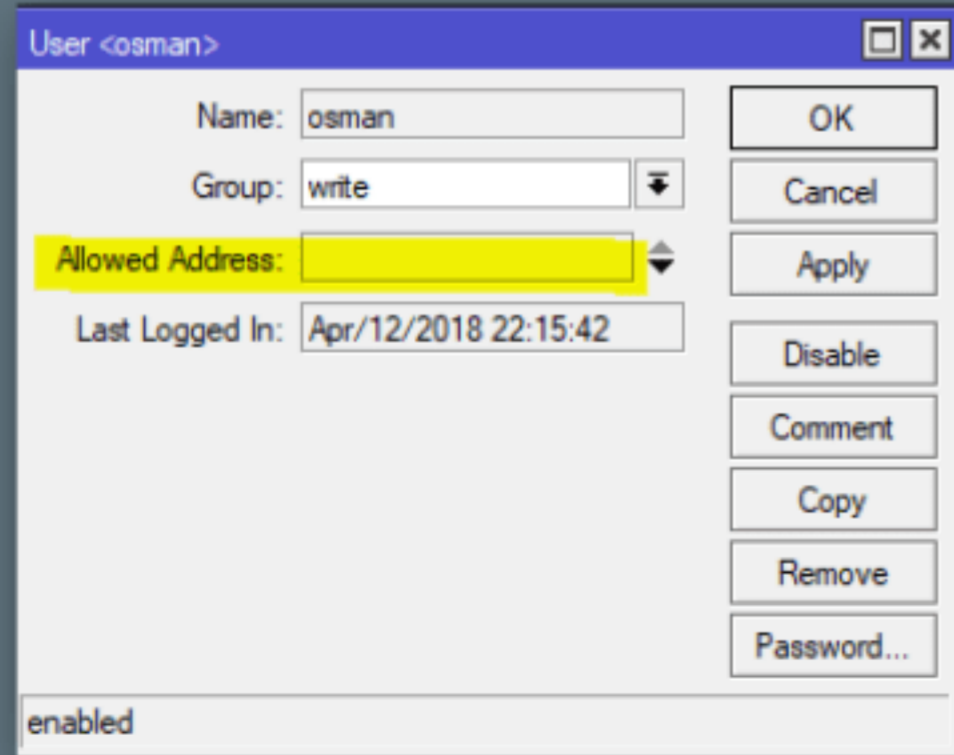
## Güncelleme

- İlk yapılması gereken RouterOS'un güncel sürümlere yükseltilmesidir.
- RouterBoot güncellemesini unutmayınız.
- Yeni güncellemeleri takip etmenizi ve changelog dokümanını incelemenizi tavsiye ediyoruz.
- <https://blog.mikrotik.com>
- [https://wiki.mikrotik.com/wiki/Manual:Securing\\_Your\\_Router#Router\\_services](https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router#Router_services)
- <https://forum.mikrotik.com>

# Kullanıcı Yönetimi



Name	Group	Allowed Address	Last Logged In
... system default user			
admin	full		Oct/12/2018 22:01:20
apiuser	read		Apr/27/2018 19:33:01
osman	write		Apr/12/2018 22:15:42
sekurim	full		Sep/18/2018 19:48:55



Name: osman

Group: write

Allowed Address: [highlighted]

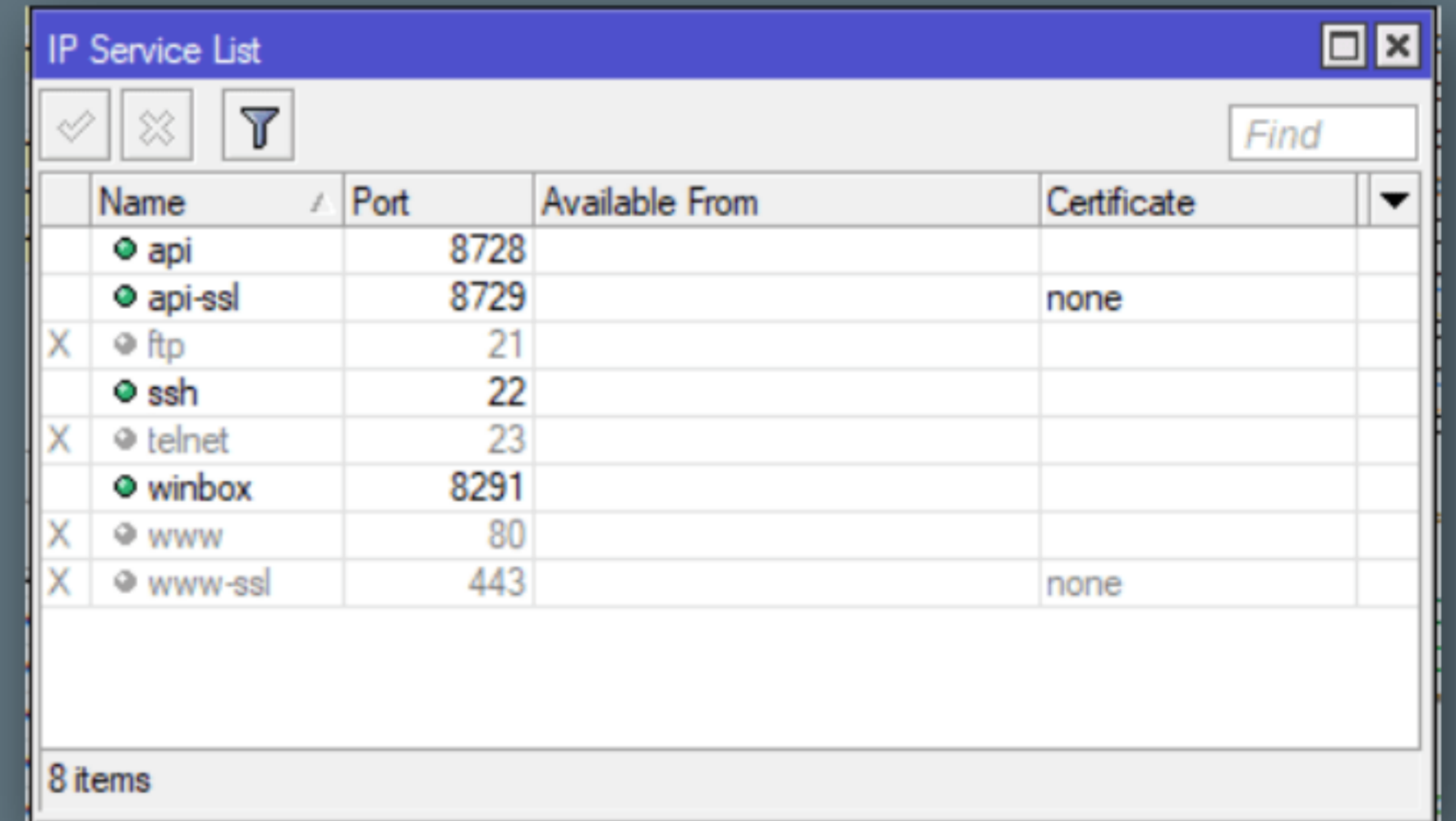
Last Logged In: Apr/12/2018 22:15:42

enabled

- admin kullanıcı adını değiştiriniz
- Tüm kullanıcılar için karmaşık şifreler kullanınız
- Grup ayarları ile yetkilendirme sistemini kullanınız. Tüm kullanıcıların ful yetki ihtiyacı var mı?
- 'Available From' ayarları ile kullanıcıların belli IP adreslerinden bağlamalarını sağlayabilirsiniz.

# IP Services

- Kullanmadığınız servisleri kapatınız
- Sadece güvenli servisleri kullanınız (ftp, telnet, www kullanmayınız.)
- API kullanmıyorsanız kapatınız

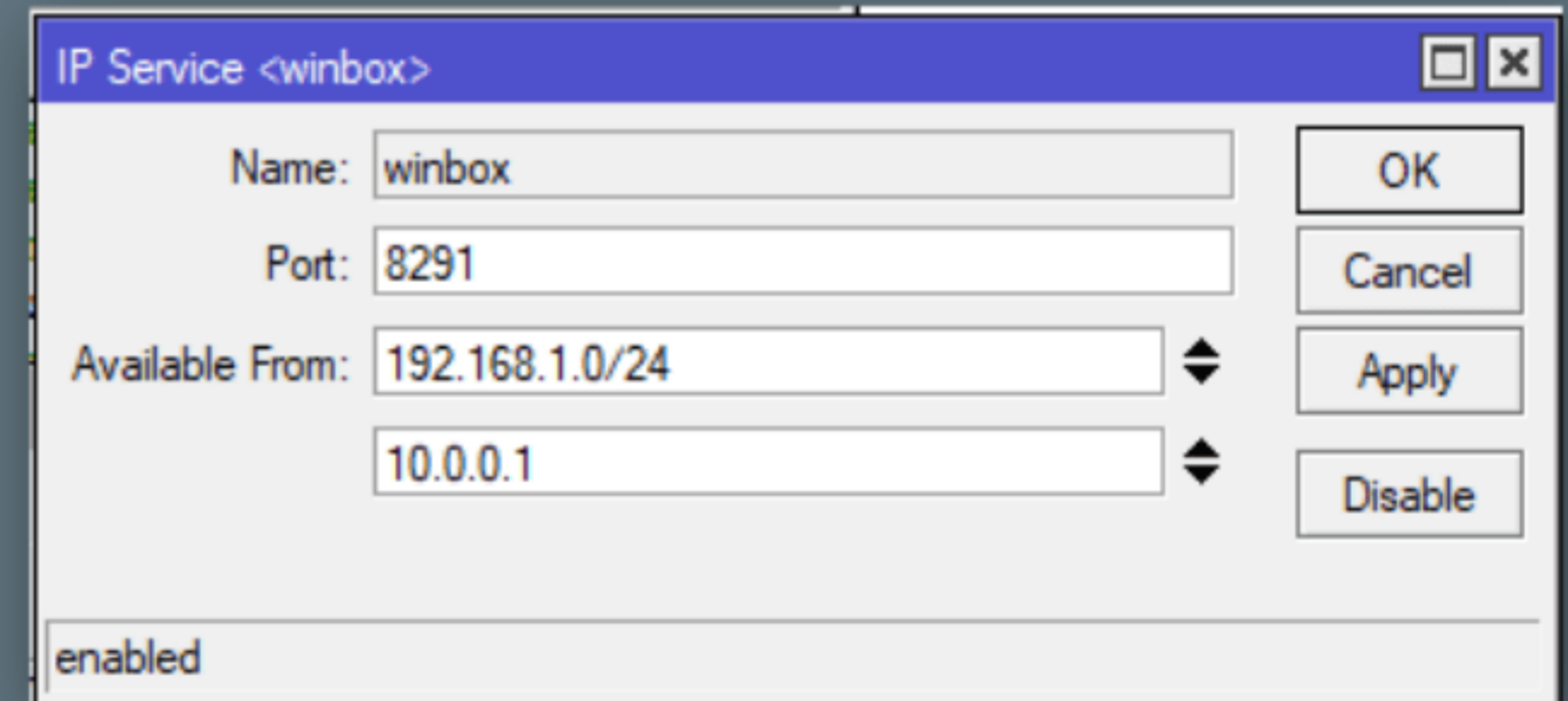


	Name	Port	Available From	Certificate	
	api	8728			
	api-ssl	8729		none	
X	ftp	21			
	ssh	22			
X	telnet	23			
	winbox	8291			
X	www	80			
X	www-ssl	443		none	

8 items

## IP Services

- 'Available From' alanını kullanınız
- Servislere hangi IP adreslerinden bağlanılabileceğini limitleyebilirsiniz.
- Servislerin çalıştığı default portları değiştirebilirsiniz.
- Bu dönemde 8291 portunu değiştirmek routerlarınızın bulunmasını engelleyecektir.

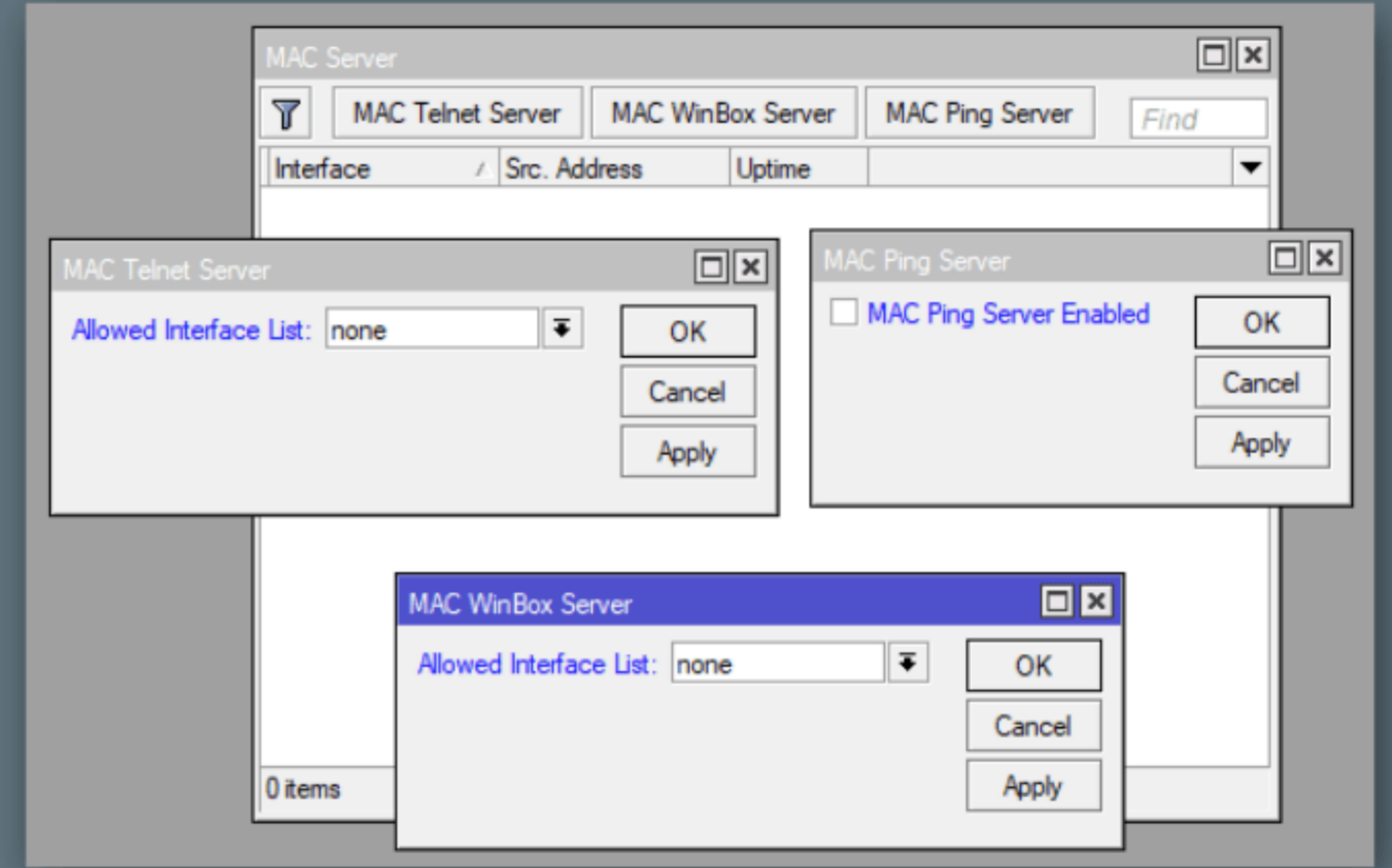


The screenshot shows a window titled "IP Service <winbox>". It contains the following fields and controls:

- Name: winbox
- Port: 8291
- Available From: 192.168.1.0/24 (with a dropdown arrow)
- 10.0.0.1 (with a dropdown arrow)
- Buttons: OK, Cancel, Apply, Disable
- Status: enabled

# MAC Eriřimi

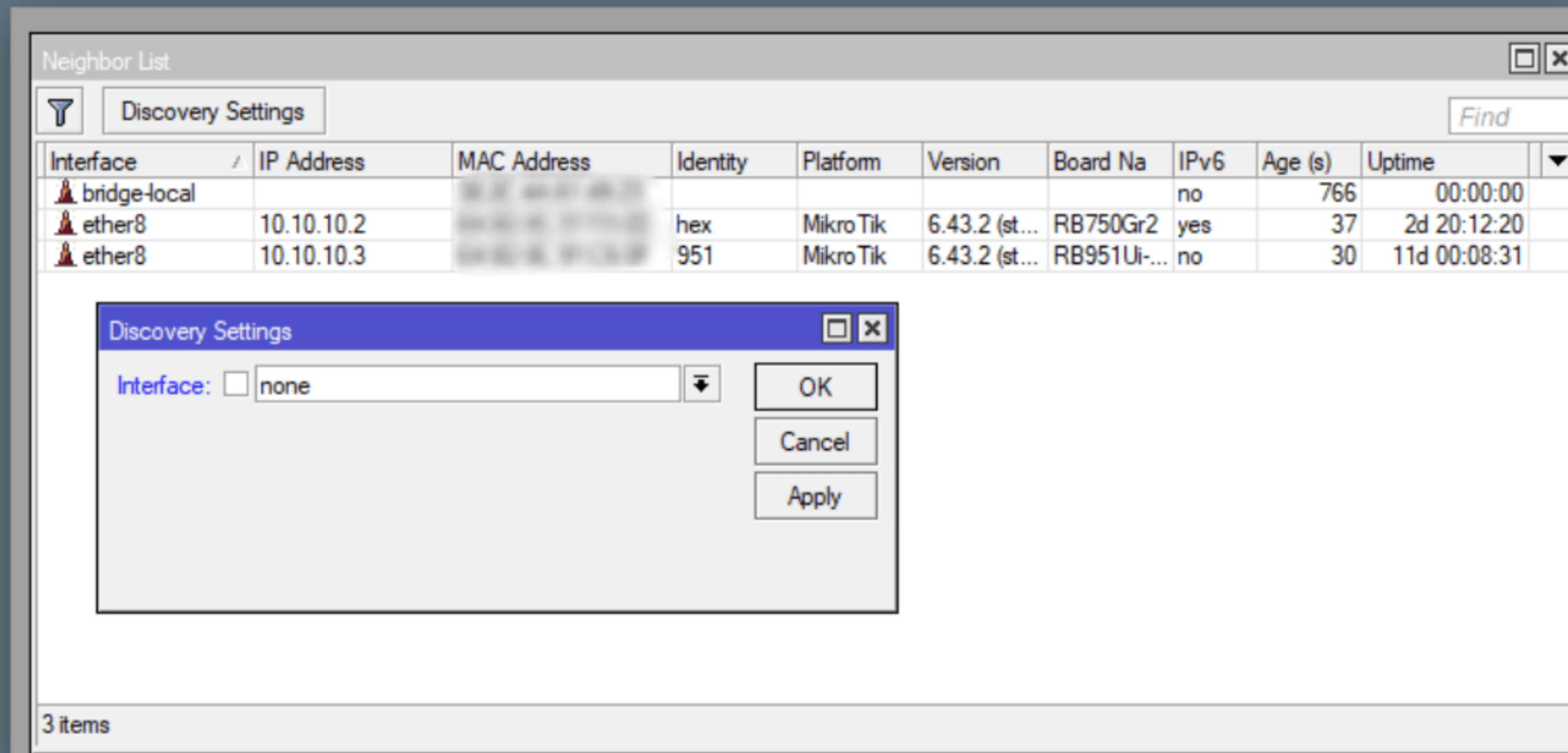
- Tüm MAC erişimleri routerlar canlı ortamda çalışırken kapatılmalıdır.
- MAC-telnet, MAC-winbox, MAC-ping servislerini kapatınız.



Tools MAC Server menüsü



# Neighbor Discovery



The screenshot shows the Mikrotik WinBox interface. The main window is titled "Neighbor List" and contains a table of discovered neighbors. A "Discovery Settings" dialog box is open in the foreground, allowing the user to select an interface for discovery. The table lists three items: a bridge-local interface, and two ether8 interfaces with IP addresses 10.10.10.2 and 10.10.10.3. The dialog box has an "Interface:" label, a dropdown menu currently set to "none", and "OK", "Cancel", and "Apply" buttons.

Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na	IPv6	Age (s)	Uptime
bridge-local							no	766	00:00:00
ether8	10.10.10.2		hex	MikroTik	6.43.2 (st...	RB750Gr2	yes	37	2d 20:12:20
ether8	10.10.10.3		951	MikroTik	6.43.2 (st...	RB951Ui...	no	30	11d 00:08:31

Discovery Settings dialog box:

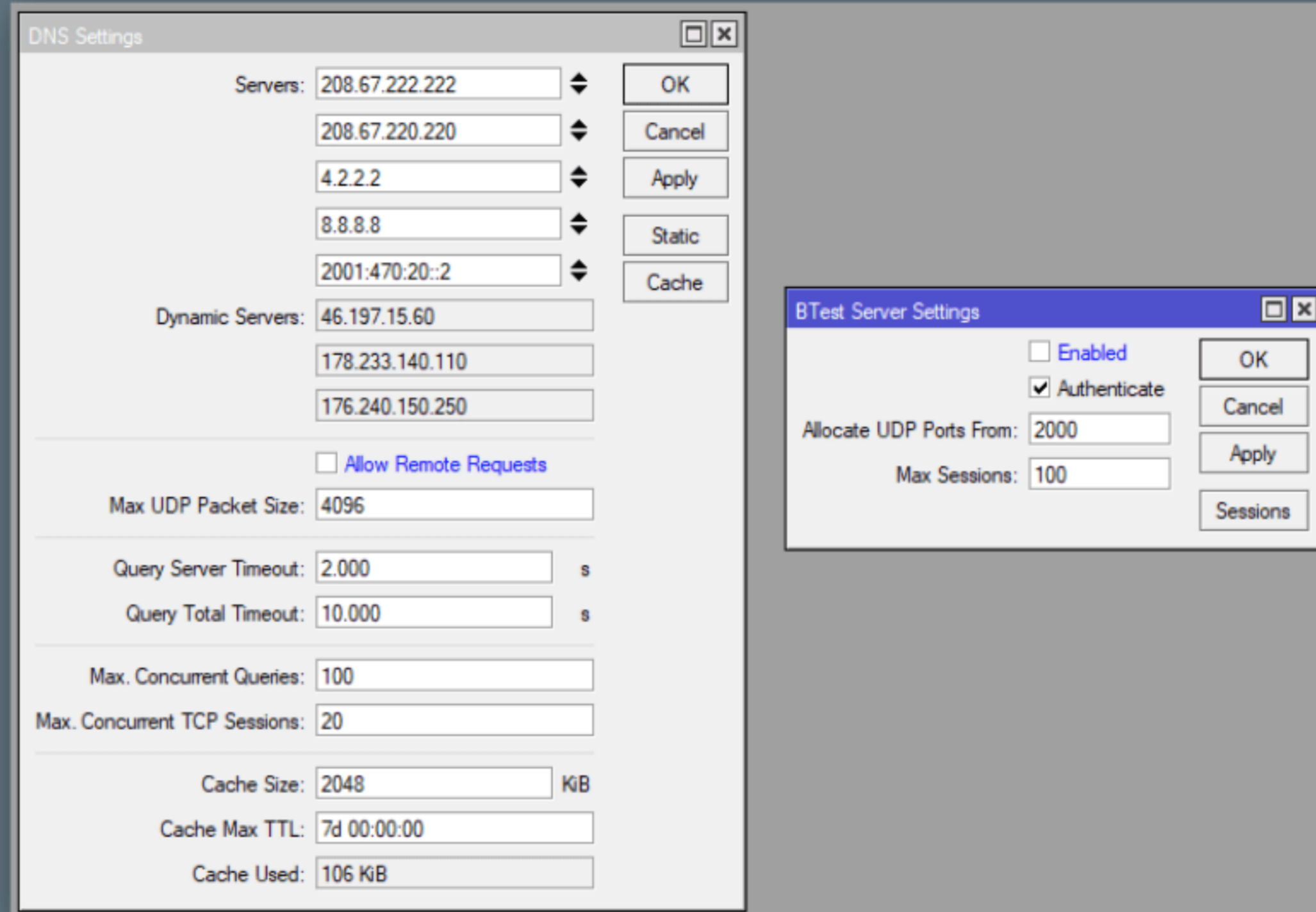
Interface:  none

Buttons: OK, Cancel, Apply

3 items

IP Neighbors Menüsü

# BW server ve DNS Cache



Tools BW server Menüsü  
IP DNS Menüsü

## SSH Erişimi

- SSH kullanılarak dosya transfer ve terminal erişimi sağlayabilirsiniz.
- SSH tünelleme kullanarak router üzerindeki diğer servislere ve router arkasındaki her türlü kaynağa bağlanabilirsiniz.
- Bu sebepten güçlü kriptoyu kullanın.
- Şifre yerine ssh anahtarları kullanabilirsiniz.

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

# SSH Tünelleme

Winbox ve router arkasındaki tüm kaynaklara ssh tünel üzerinden erişilebilir

```
C:\Users\merlyn
λ ssh admin@192.168.1.157 -L 8291:localhost:8291
admin@192.168.1.157's password:

MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTT      KKK
MMM MMMM MMM III  KKK KKK RRRRRR  000000  TTT  III  KKK KKK
MMM MM  MMM III  KKKKK  RRR  RRR  000  000  TTT  III  KKKKK
MMM  MMM III  KKK KKK  RRRRRR  000  000  TTT  III  KKK KKK
MMM  MMM III  KKK KKK  RRR  RRR  000000  TTT  III  KKK KKK

MikroTik RouterOS 6.41 (c) 1999-2017      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]        Completes the command/word. If the input is ambiguous,
              a second [Tab] gives possible options

/            Move up to base level
..          Move up one level
/command    Use command at the base level

[admin@sekuritim] > |
```

WinBox v3.17 (Addresses)

File Tools

Connect To:

Login:

Password:

Session:

Note:

Group:

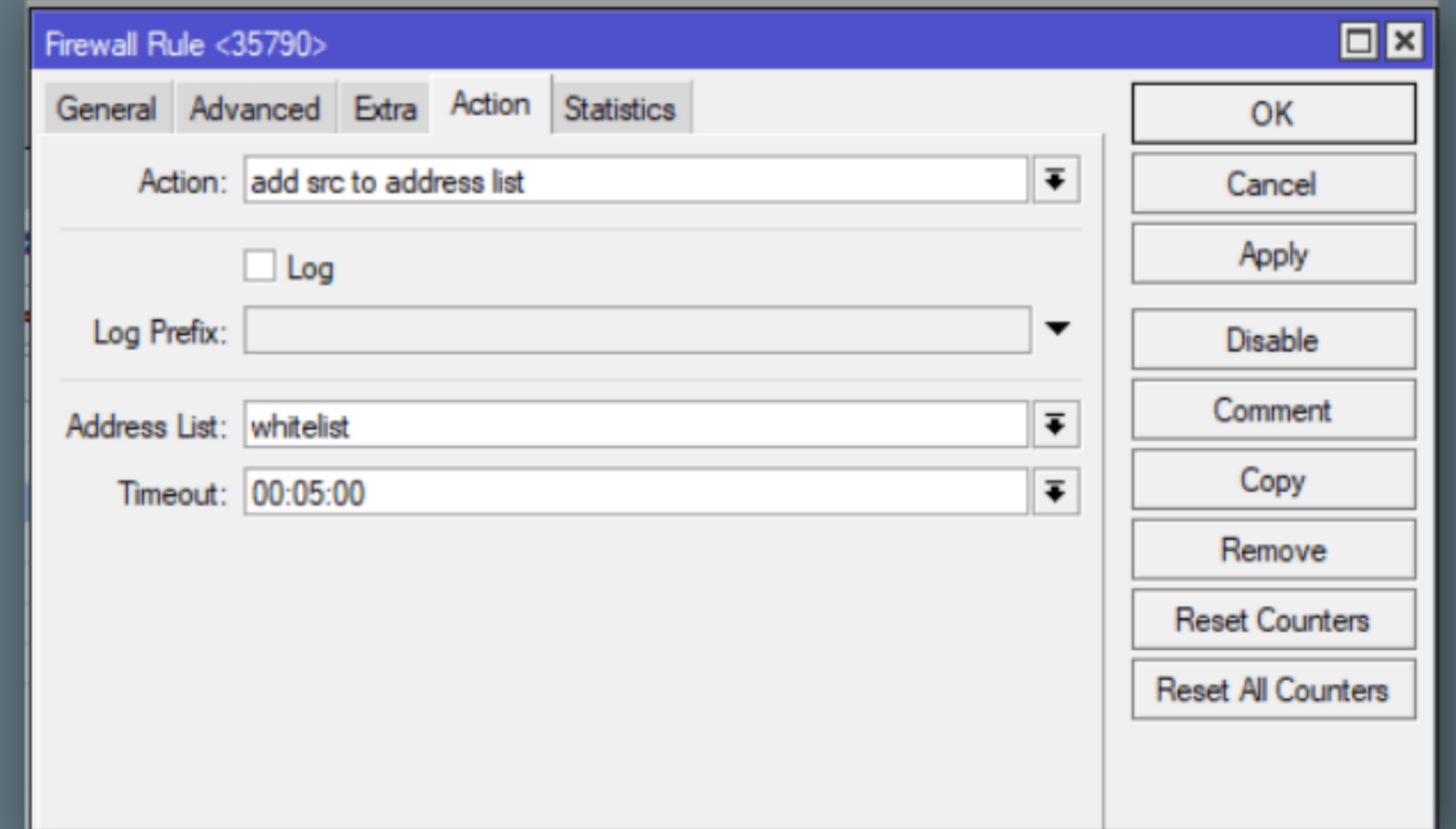
RoMON Agent:

## Firewall

- Firewall yükünü azaltmak için sadece 'new' paketleri filtreleyen kurallar uygulayınız.
- 'Established' ve 'related' kurallarını uygulayınız.
- 'Invalid' Paketleri drop ediniz.
- Sadece gerekli trafiğe izin veriniz. Geri kalan herşeyi drop ediniz.
- Firewall kurallarında comment kullanınız.
- Router'ın herhangi bir servis portu internete açılmamalıdır.
- Servislere 3 hatalı denemede otomatik bloklama ayarlanabilir.

# Port Knocking

- Router'a özel bir paket göndererek geçici süreliğine erişim açılmasını sağlayabilirsiniz.
- Paket boyutu, port numaraları, paket içeriği kullanılarak özel paket oluşturulabilir.
- Birden fazla paket ile port knocking ayarlanabilir.



The screenshot shows the 'Firewall Rule <35790>' configuration window. The 'Action' tab is selected, showing the following settings:

- Action: add src to address list
- Log:
- Log Prefix: (empty)
- Address List: whitelist
- Timeout: 00:05:00

On the right side, there are several buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

# Port Scan Detection

Firewall

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

+ - ✓ ✕ [icon] [icon] 00 Reset Counters 00 Reset All Counters

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port
::: Port Scanning check						
32	add src to address list	PortScan			6 (tcp)	

Firewall Rule <>

General Advanced Extra Action Statistics

Connection Limit

Limit

Dst. Limit

Nth

Time

Src. Address Type

Dst. Address Type

PSD

Weight Threshold: 21

Delay Threshold: 00:00:03

Low Port Weight: 3

High Port Weight: 1

Hotspot

IP Fragment

# Firewall Kuralları

#	Action	Chain	Src. Address	Dst. Address	Proto	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets	
::: INVALID DROP												
0	✗ drop	input								1051 B	13	
::: ESTABLISHED RELATED ACCEPT												
1	✓ acc	input								1504.7 KiB	4 348	
::: PSD												
2	➡ add...	forward			6 (tcp)					132 B	3	
::: Portknocking												
3	➡ add...	input			6 (tcp)		35790			0 B	0	
::: WHITELIST												
4	✓ acc	input								1153.7 KiB	17 836	
::: PSD												
5	↔ jump	input			6 (tcp)					1280 B	26	
::: Service Attack												
6	↔ jump	input			6 (tcp)		21,22,23,...			460 B	9	
::: DEFAULT DROP												
7	✗ drop	input								14.8 KiB	245	
::: blacklist brute force												
8	➡ add...	Service_at...			6 (tcp)		21,22,23,...			0 B	0	
::: brute force attempt#3												
9	➡ add...	Service_at...			6 (tcp)		21,22,23,...			104 B	2	
::: brute force attempt#2												
10	➡ add...	Service_at...			6 (tcp)		21,22,23,...			260 B	5	
::: brute force attempt#1												
11	➡ add...	Service_at...			6 (tcp)		21,22,23,...			460 B	9	
12	➡ add...	PSD			6 (tcp)					44 B	1	

13 items



# RPFilter

IP Settings

IP Forward

Send Redirects

Accept Redirects

Secure Redirects

Accept Source Route

Allow Fast Path

Route Cache

RP Filter:  ▾

TCP SynCookies

Max Neighbor Entries:

ARP Timeout:

ICMP Rate Limit:

IPv4 Fast Path Active

IPv4 Fast Path Packets:

IPv4 Fast Path Bytes:

IPv4 Fasttrack Active

IPv4 Fasttrack Packets:

IPv4 Fasttrack Bytes:

OK

Cancel

Apply

## Son Önerilerimiz

- Kendi güvenlik standartlarınızı ve güvenlik yapılandırmalarınızı oluşturunuz.
- Standartlarınızı tüm routerlara uygulayınız.
- Trafik analizi ve bir SIEM sistemi saldırıları önceden tespit etmek için çok yararlı olacaktır.
- Log izleme scriptini inceleyiniz.
- [https://wiki.mikrotik.com/wiki/Monitor\\_logs,\\_send\\_email\\_alert/\\_run\\_script](https://wiki.mikrotik.com/wiki/Monitor_logs,_send_email_alert/_run_script)



## Teşekkürler

Sunuma linkten ulaşabilirsiniz.

<https://app.slidebean.com/p/HcmB8EKo1m/RouterOS-Gvenlii>