

RouterOS Güvenliđi

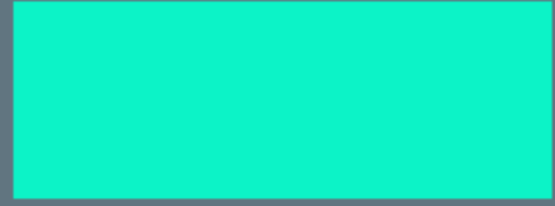
MUM İstanbul 2018

Osman Kazdal



Sekuritim Bilişim

MikroTik
ROUTING THE WORLD



Ben Kimim?

Osman Kazdal

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

Sekuritim Biliřim

- Value Added Master Distributor
- Eđitim Merkezi
- Danıřmanlık
- Kurulum
- Destek
- 2008 yılında kurulmuřtur.
- Atařehir İstanbul



İletişim

- Email: 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

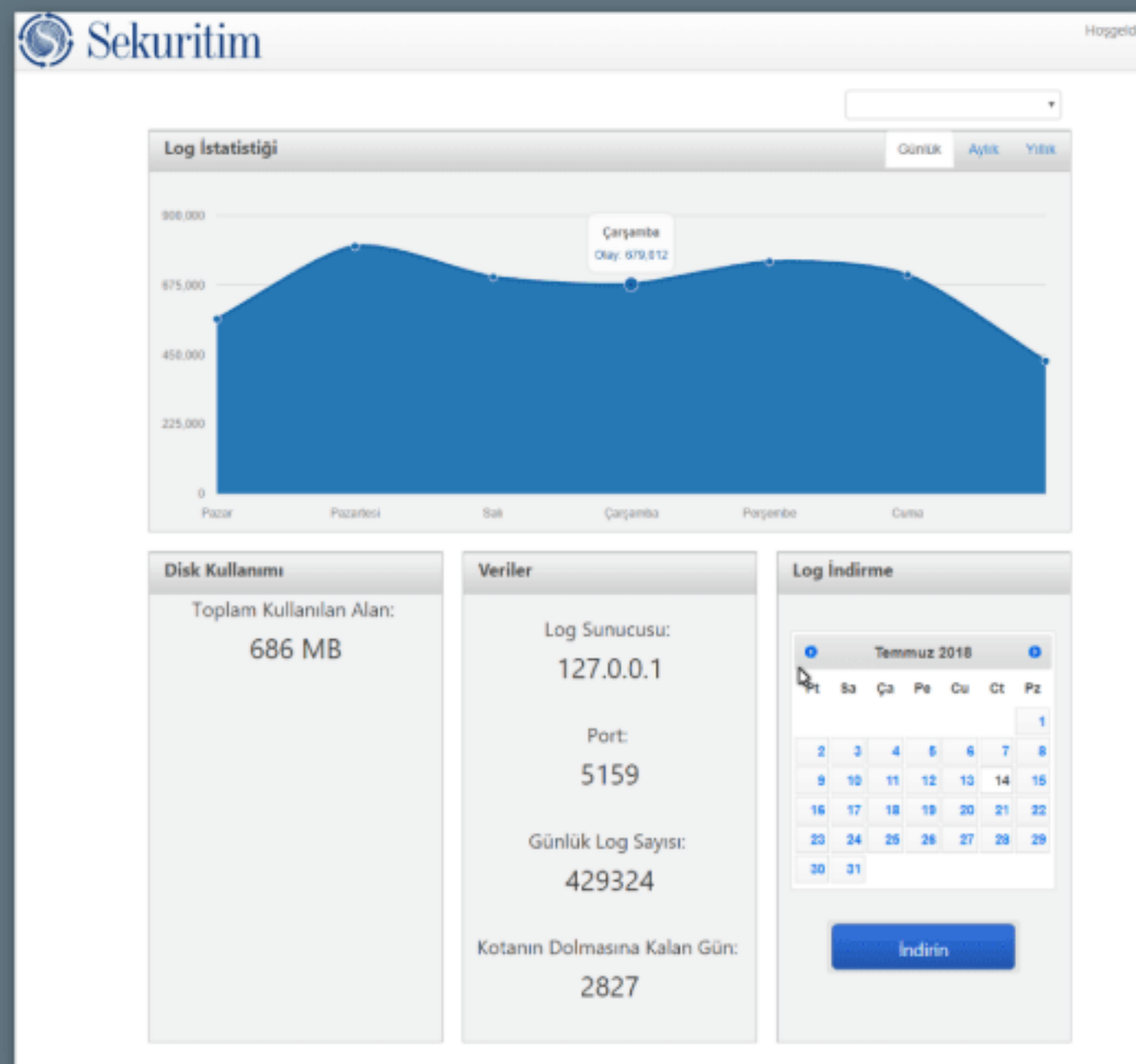


Standımıza Bekliyoruz



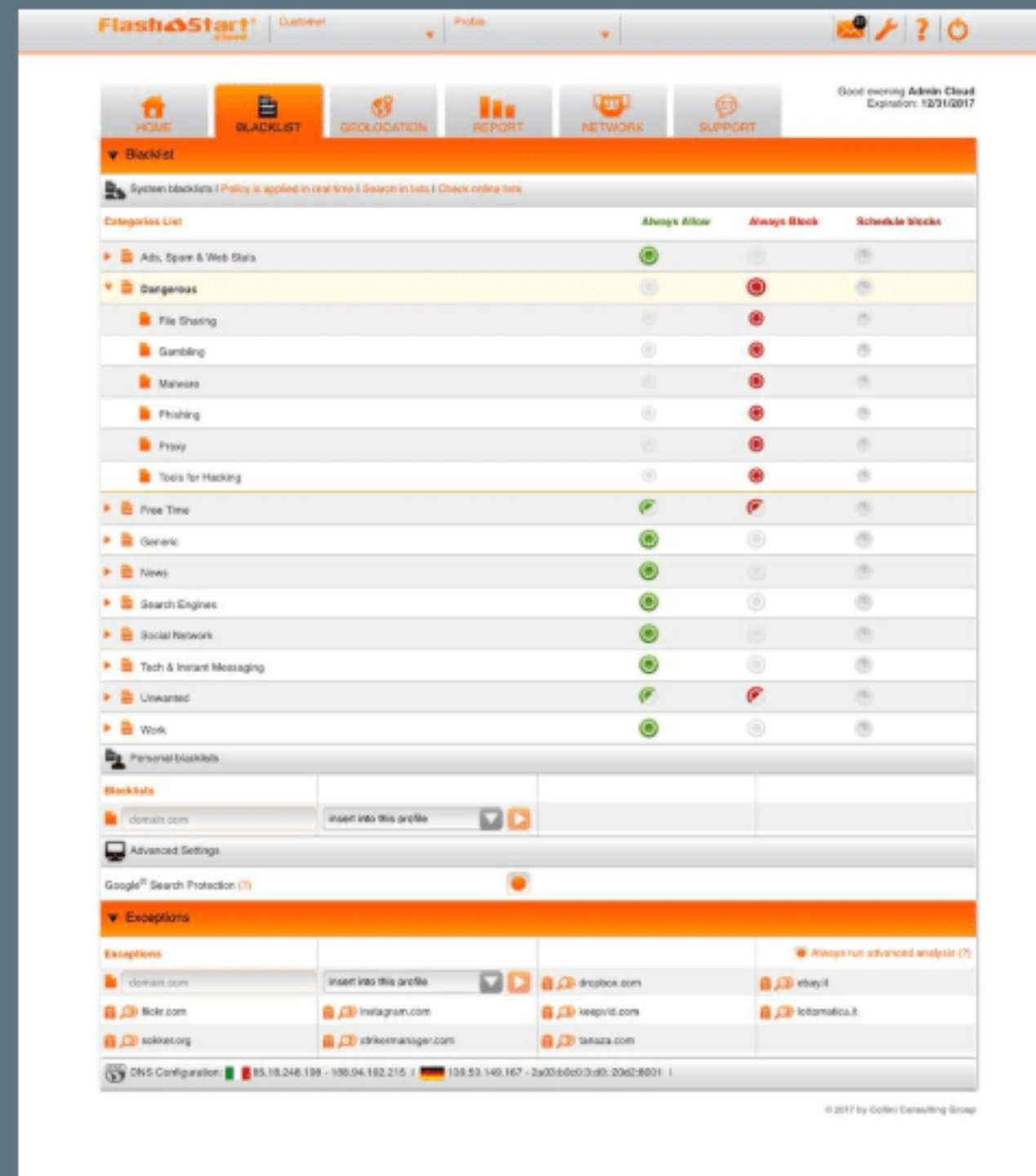
LTE Ürünleri





The screenshot shows a Windows desktop environment. In the foreground, a window titled 'Kamu Sertifikasyon Merkezi' (You Certification Center) is open. It displays a digital certificate for the file '20170315.log'. The certificate is issued by 'TCL SvastLnD4YpnV63DR8JnVfVfHsFz9Q9CstTuzo=' on 16 March 2017 at 01:00:02 GMT. The certificate is valid for 365 days and is signed by the same entity. The background shows a file explorer window with a list of files, including '20170315.log' and '20170315.log.txt'. The desktop also has several icons, including 'DUDE-1036...', 'OSPF-Main...', 'Avast Premier', and 'Zaman 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

The Sony logo, featuring the word "SONY" in a bold, blue, sans-serif font.The TEB Yatırım logo, featuring a green square with three white stars and the text "TEB YATIRIM" in black.The Panço logo, featuring the word "PANÇO" in a stylized, purple, sans-serif font with a registered trademark symbol.The Çayla logo, featuring the word "Çayla" in a black, sans-serif font with a red floral emblem.The Turkcell Superonline logo, featuring the word "TURKCELL" in blue and "SUPERONLINE" in red.The Vodafone logo, featuring a red speech mark icon and the word "vodafone" in red.



RouterOS Güvenliği

Nasıl saldırıyorlar?

Neden saldırıyorlar?

Kendimizi nasıl koruruz?

Demo



Saldırının Aşamaları

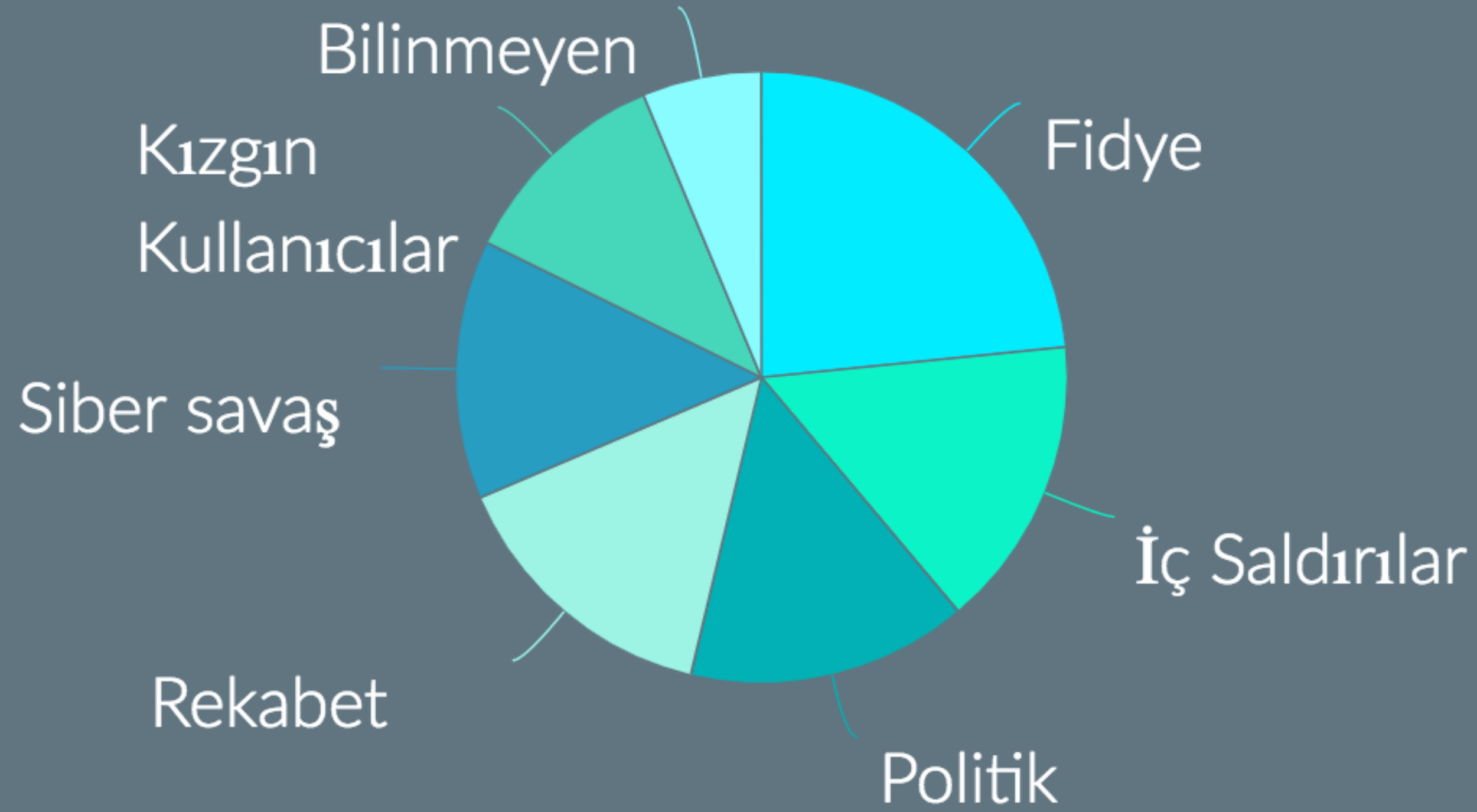
- Port tarama ile MikroTik router tespit edilmesi
- Winbox açışının kullanılarak şifrelerin ele geçirilmesi
- Router'ın ele geçirilmesi

Ne yaptılar?

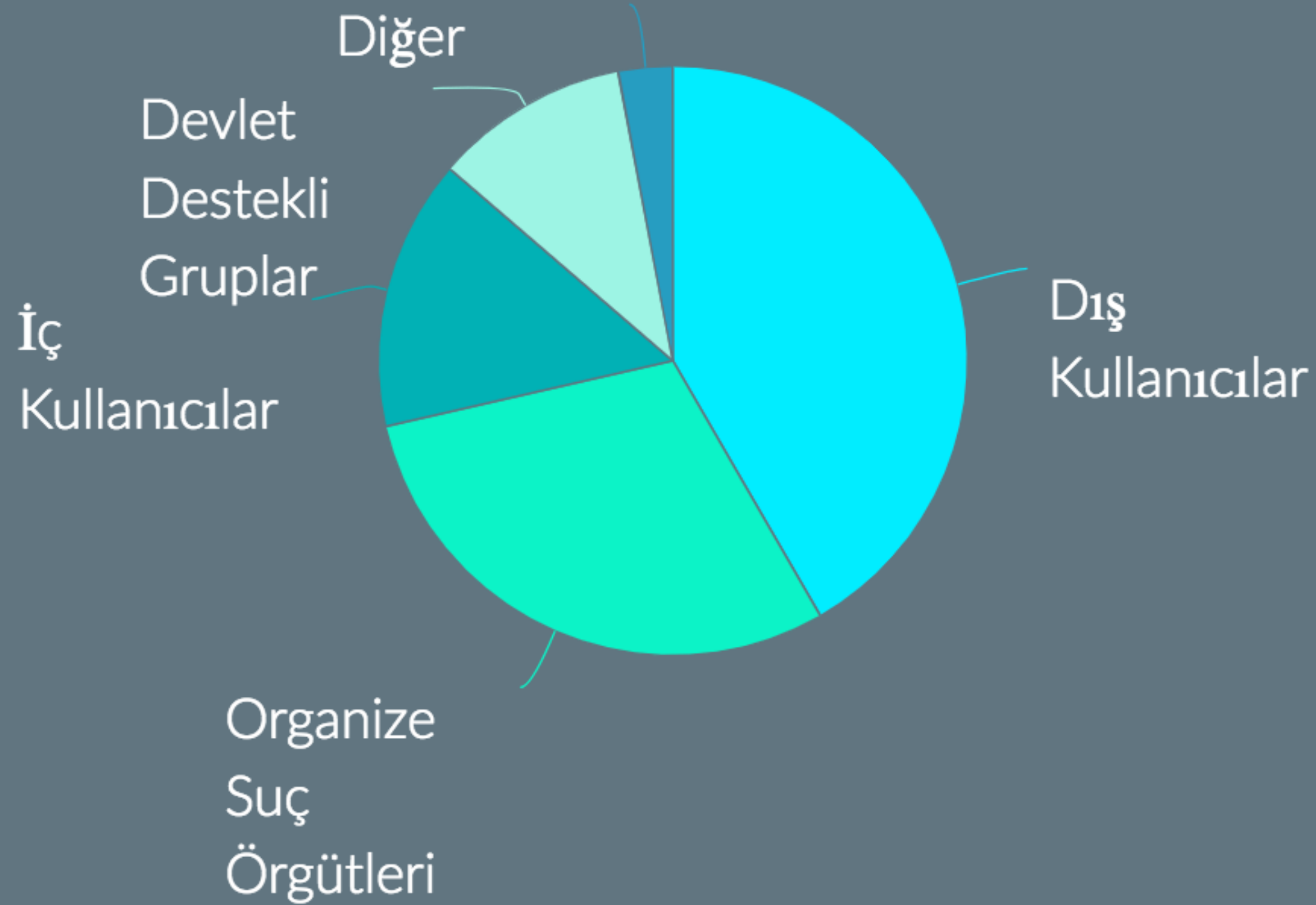
```
/ip firewall filter
add action=tarpit chain=input comment="Add you ip address to allow-ip in Address Lists." dst-port=30553 protocol=tcp
add action=add-src-to-address-list address-list=allow-ip address-list-timeout=1h chain=input comment="The security flaw for Hajime is closed by the firewall." packet-size=1083 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?

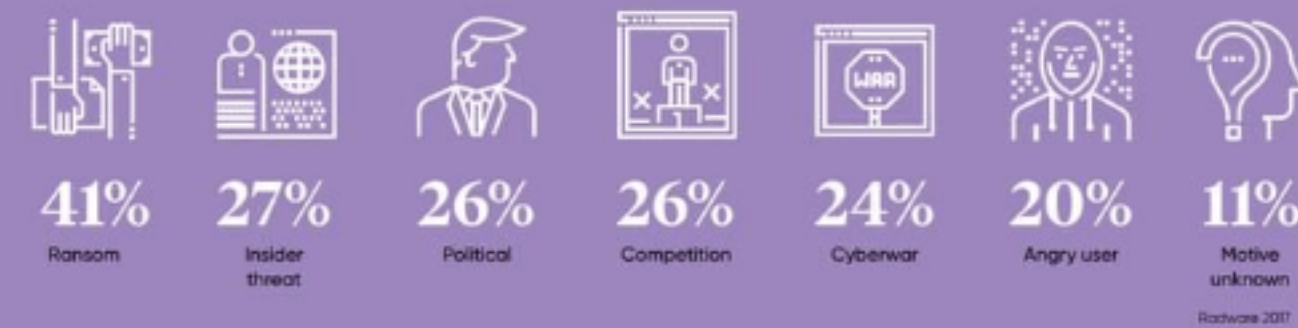


Infograph

WHY HACKERS HACK

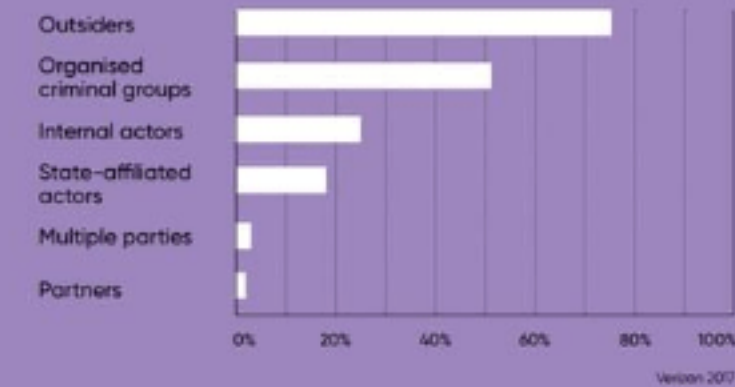
MOTIVES BEHIND CYBERATTACKS

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



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



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 filtrelenmelidir

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: 98:1B:4D:8E:3A:25 (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 Validation
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

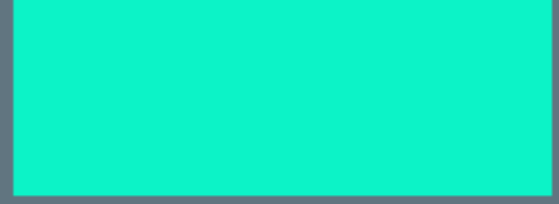
- Brute force şifre saldırıları
- Winbox açığı kullanıldığında şifre saldırıları yapmadan şifreler açığa çıktı.
- Şifre saldırılarına karşı karmaşık şifreler kullanılmalıdır
- IP Firewall ve IP services ayarlarından router'a bağlanabilecek IP adresleri kısıtlanmalıdır.



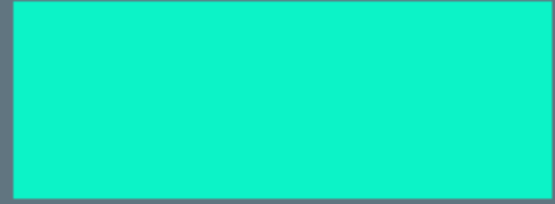
DoS & DDoS Saldırıları

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.



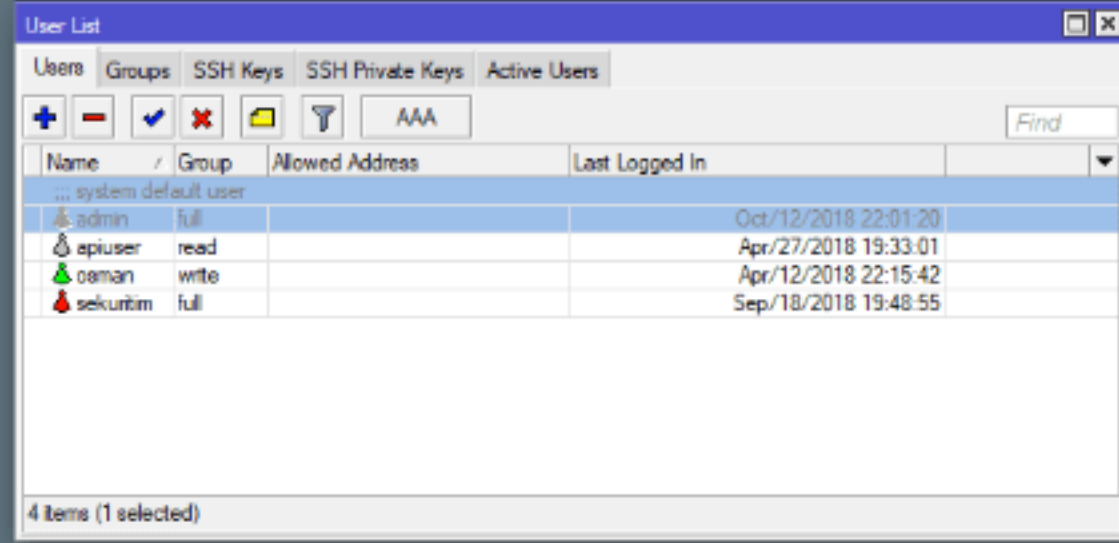
Ne Yapacağız?



Güncelleme

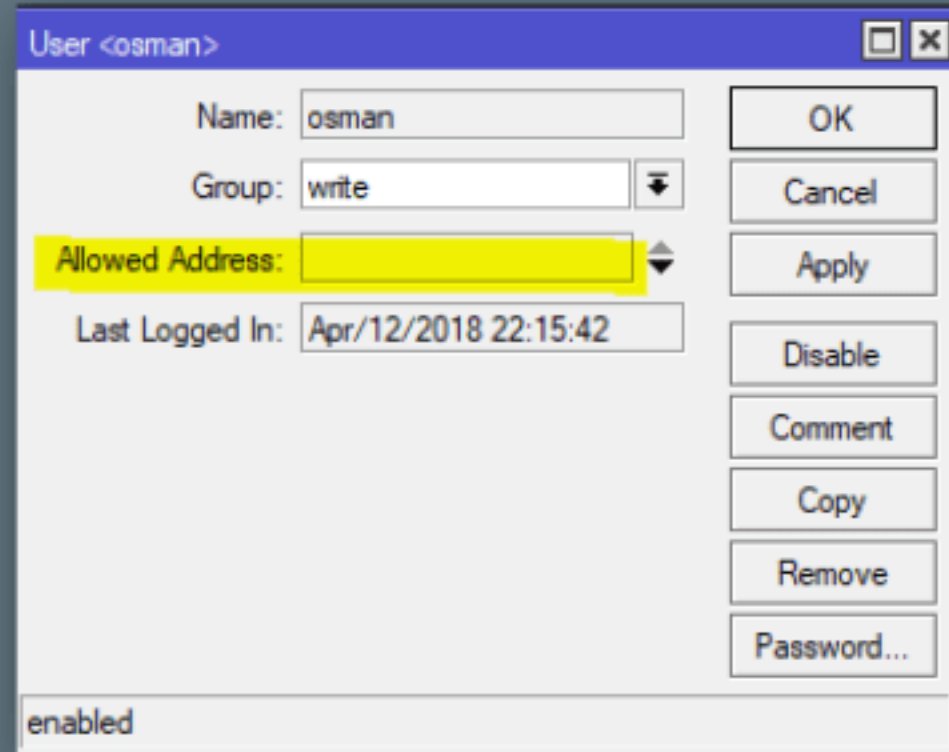
- İlk yapılması gereken RouterOS'un güncel sürümlere yükseltilmesidir.
- RouterBoot güncellemesini unutmayınız.
- Yeni güncellemeleri takip etmenizi ve changelog dokümanının incelemenizi tavsiye ediyoruz.
- <https://blog.mikrotik.com>
- https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router#Router_services
- <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

4 items (1 selected)



User <osman>

Name: osman

Group: write

Allowed Address:

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

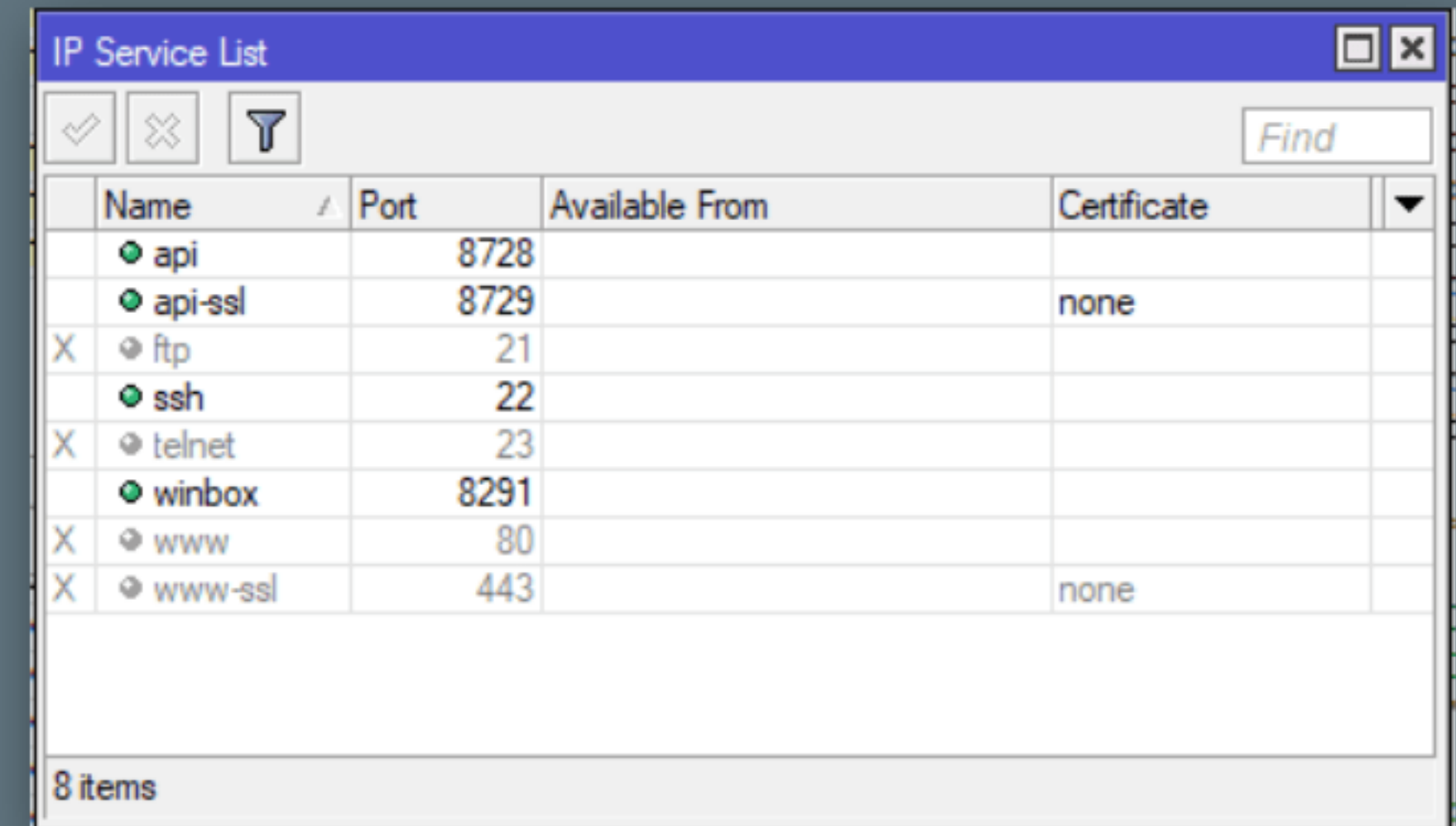
enabled

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Password...

- 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



The screenshot shows a window titled "IP Service List" with a table of services. The table has columns for Name, Port, Available From, and Certificate. The services listed are api, api-ssl, ftp, ssh, telnet, winbox, www, and www-ssl. The status of each service is indicated by a green dot (on) or a red X (off). The certificate status is shown in the Certificate column, with "none" for api-ssl and www-ssl.

	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.

IP Service <winbox>

Name: winbox

Port: 8291

Available From: 192.168.1.0/24

10.0.0.1

OK

Cancel

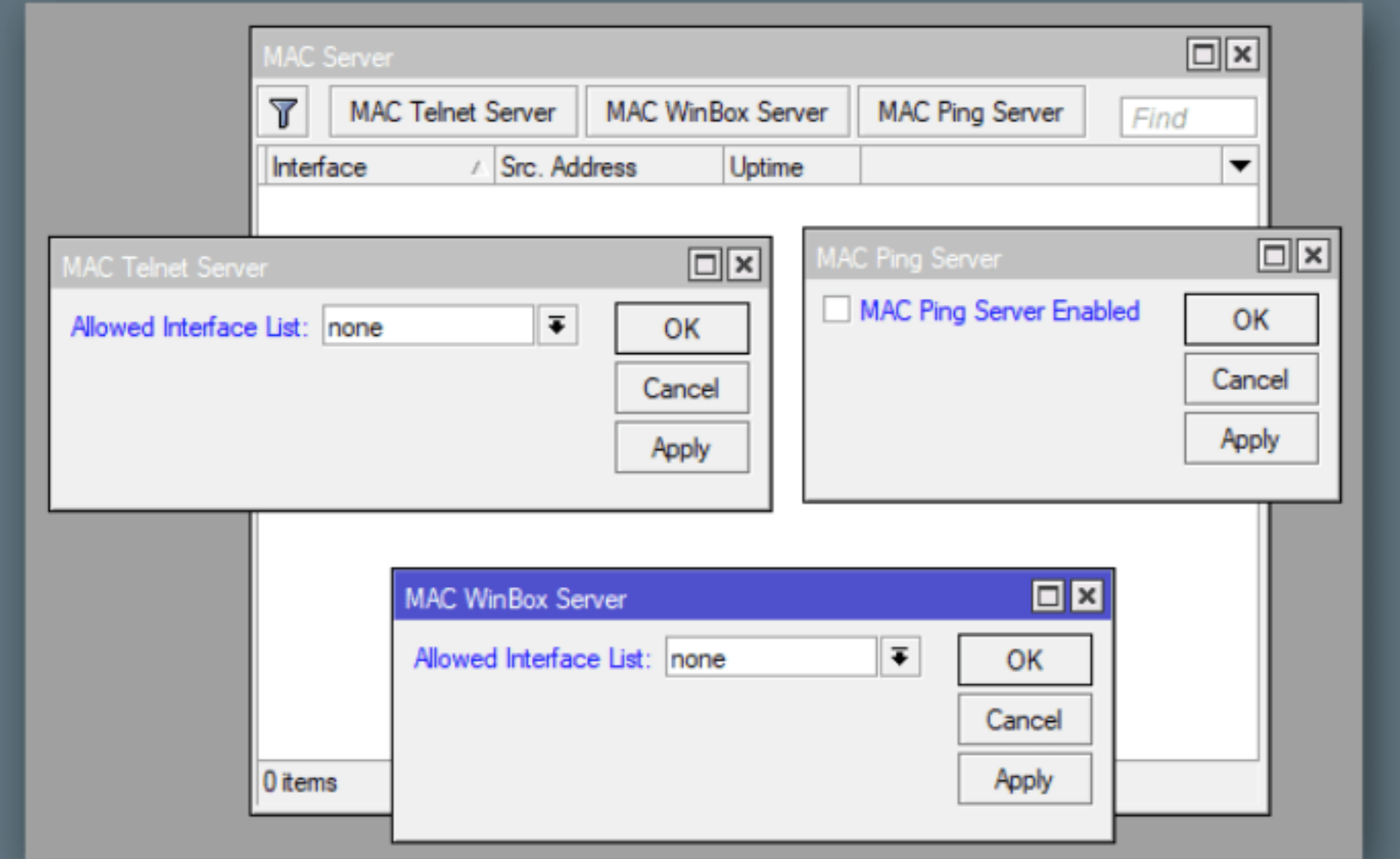
Apply

Disable

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

Neighbor List

Discovery Settings Find

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	Mikro Tik	6.43.2 (st...	RB750Gr2	yes	37	2d 20:12:20
ether8	10.10.10.3		951	Mikro Tik	6.43.2 (st...	RB951Ui...	no	30	11d 00:08:31

Discovery Settings

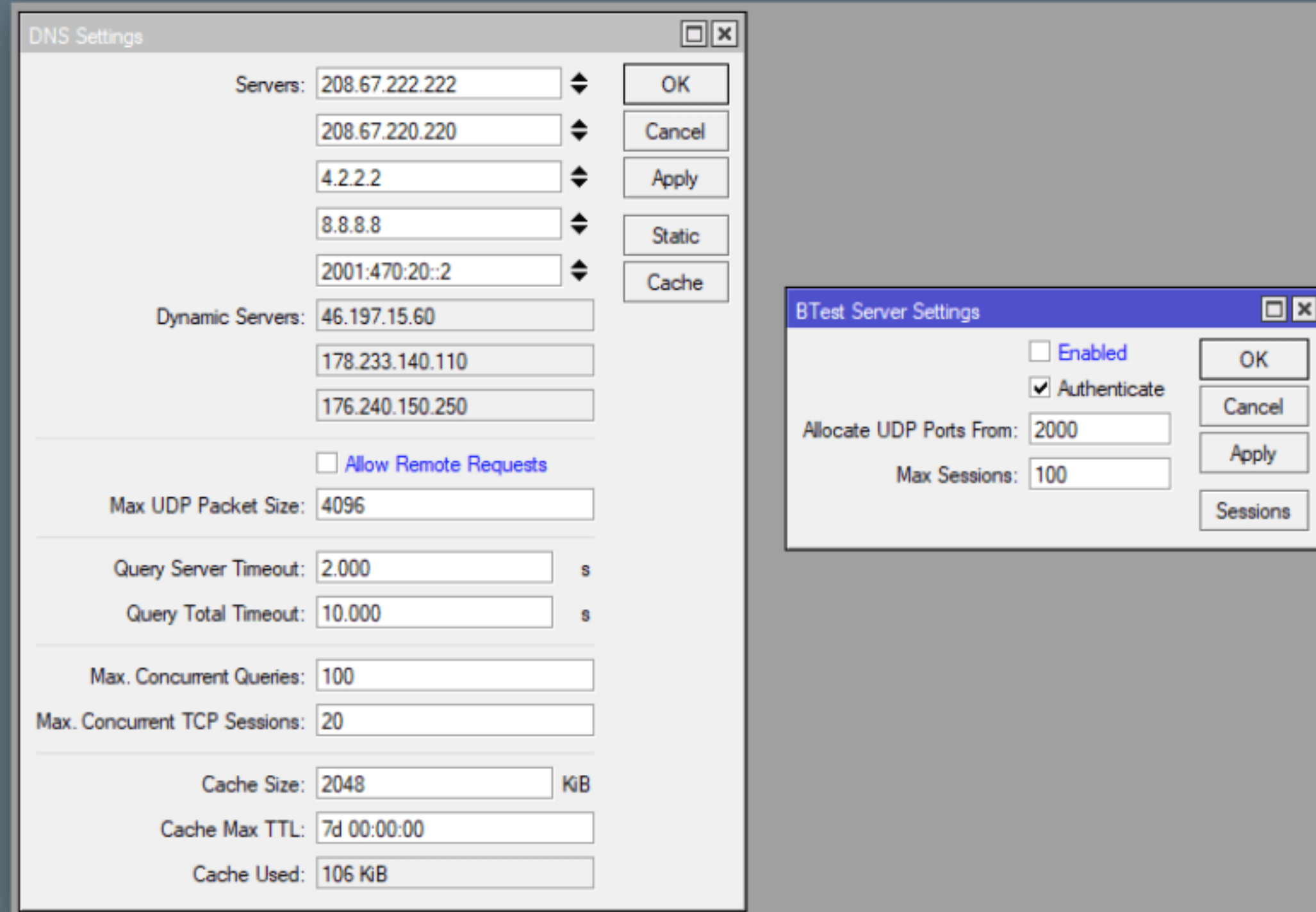
Interface: ☐ none

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 kriptu kullanınız.
- 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: 127.0.0.1

Login: admin

Password: *****

Session: <own>

Note: AWS

Group: SEKURITIM

RoMON Agent:

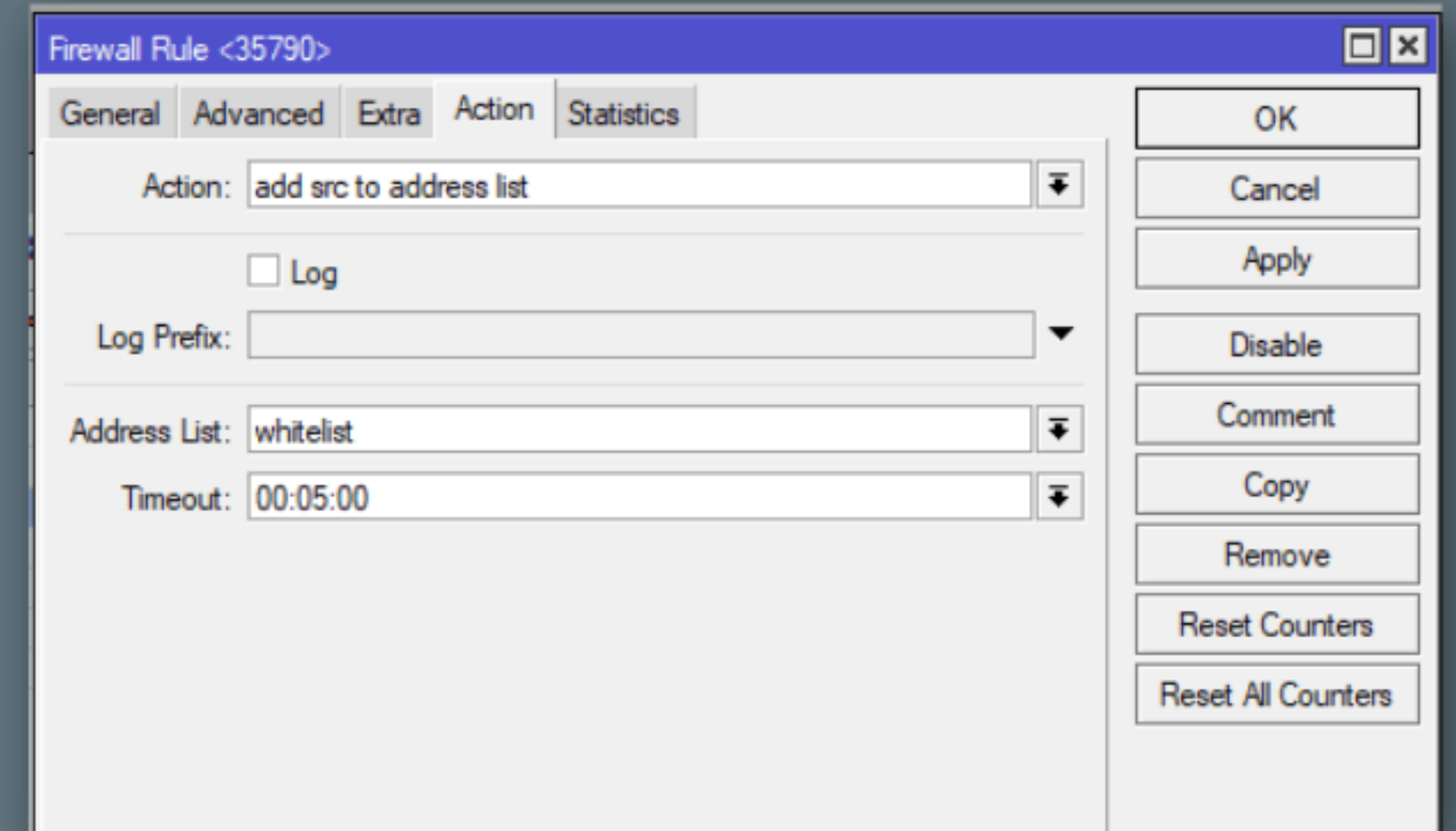
Add/Set

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 'General' tab is selected. The 'Action' dropdown is set to 'add src to address list'. The 'Log' checkbox is unchecked. The 'Log Prefix' field is empty. The 'Address List' dropdown is set to 'whitelist'. The 'Timeout' field is set to '00:05:00'. On the right side, there are buttons for '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] 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

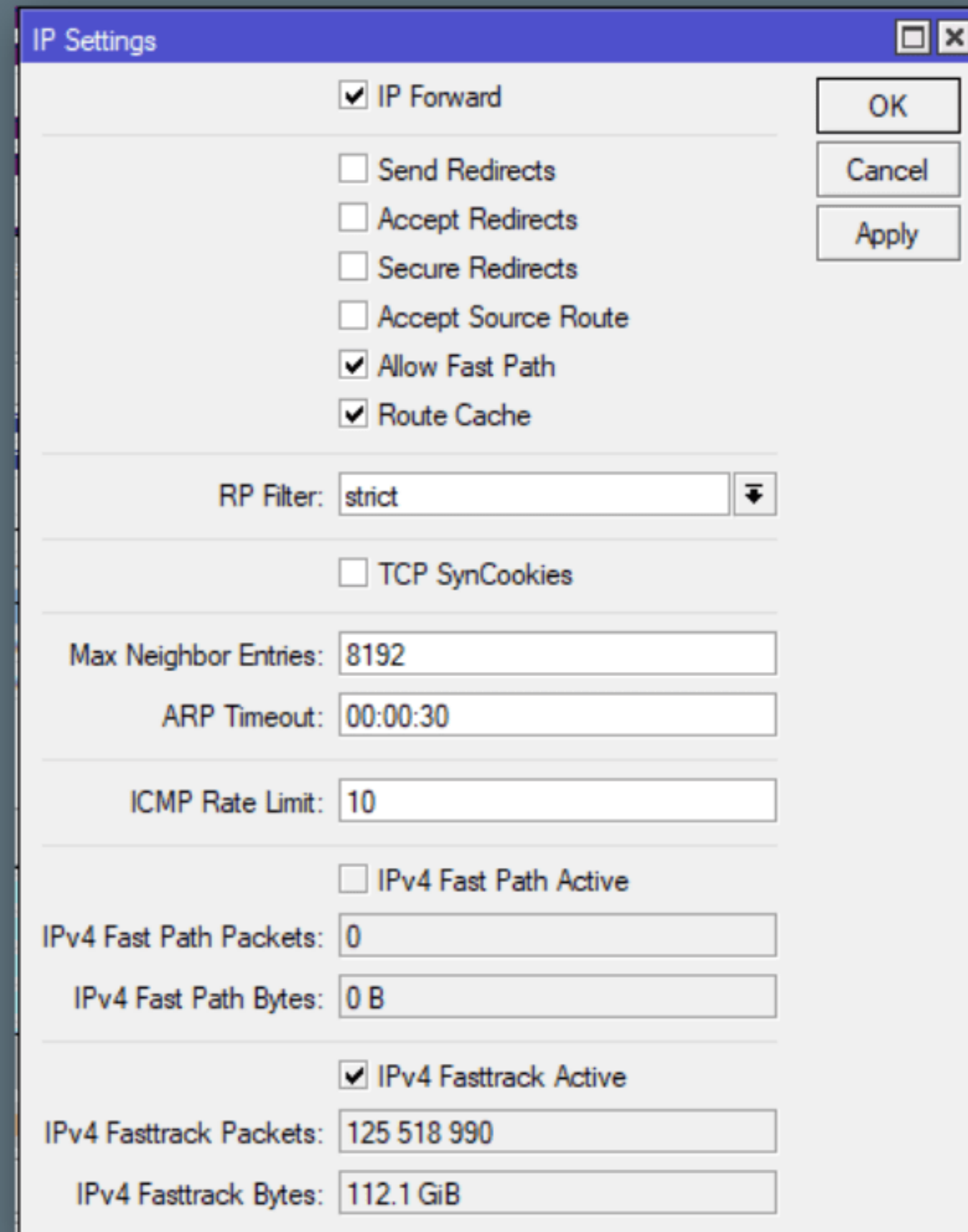
High Port Weight: 1

Hotspot

IP Fragment

[illegible]

RPFilter



The image shows a screenshot of the Windows 'IP Settings' dialog box. The window has a blue title bar with the text 'IP Settings' and standard window controls (minimize, maximize, close). The main area contains several sections of settings, each separated by a horizontal line. The first section contains checkboxes for 'IP Forward' (checked), 'Send Redirects' (unchecked), 'Accept Redirects' (unchecked), 'Secure Redirects' (unchecked), 'Accept Source Route' (unchecked), 'Allow Fast Path' (checked), and 'Route Cache' (checked). To the right of these checkboxes are three buttons: 'OK', 'Cancel', and 'Apply'. The second section has a label 'RP Filter:' followed by a text box containing 'strict' and a dropdown arrow. The third section contains a checkbox for 'TCP SynCookies' (unchecked). The fourth section contains three text boxes: 'Max Neighbor Entries:' with the value '8192', 'ARP Timeout:' with the value '00:00:30', and 'ICMP Rate Limit:' with the value '10'. The fifth section contains a checkbox for 'IPv4 Fast Path Active' (unchecked), followed by two text boxes: 'IPv4 Fast Path Packets:' with the value '0' and 'IPv4 Fast Path Bytes:' with the value '0 B'. The sixth section contains a checkbox for 'IPv4 Fasttrack Active' (checked), followed by two text boxes: 'IPv4 Fasttrack Packets:' with the value '125 518 990' and 'IPv4 Fasttrack Bytes:' with the value '112.1 GiB'.

IP Settings

☒ IP Forward

☐ Send Redirects

☐ Accept Redirects

☐ Secure Redirects

☐ Accept Source Route

☒ Allow Fast Path

☒ Route Cache

RP Filter: strict

☐ TCP SynCookies

Max Neighbor Entries: 8192

ARP Timeout: 00:00:30

ICMP Rate Limit: 10

☐ IPv4 Fast Path Active

IPv4 Fast Path Packets: 0

IPv4 Fast Path Bytes: 0 B

☒ IPv4 Fasttrack Active

IPv4 Fasttrack Packets: 125 518 990

IPv4 Fasttrack Bytes: 112.1 GiB

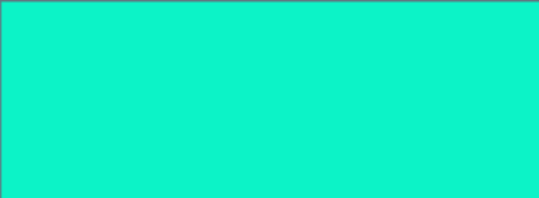
OK

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>