Reducing the impact of DoS attacks with MikroTik RouterOS

Alfredo Giordano
Matthew Ciantar

TikTrain.com

About Us

Alfredo Giordano

MikroTik Certified Trainer and Consultant

Support deployment of WISP Providers

Internet Bandwidth Provider

From Italy

Matthew Ciantar

Advanced MikroTik User since 2002

MikroTik Certified Trainer and Consultant

Works in the Betting Industry

From Malta, located in Dublin, Ireland

Providing professional and specialised MikroTik Training Classes in varies languages, as well as Consultancy Services under the TikTrain.com brand since March 2014.

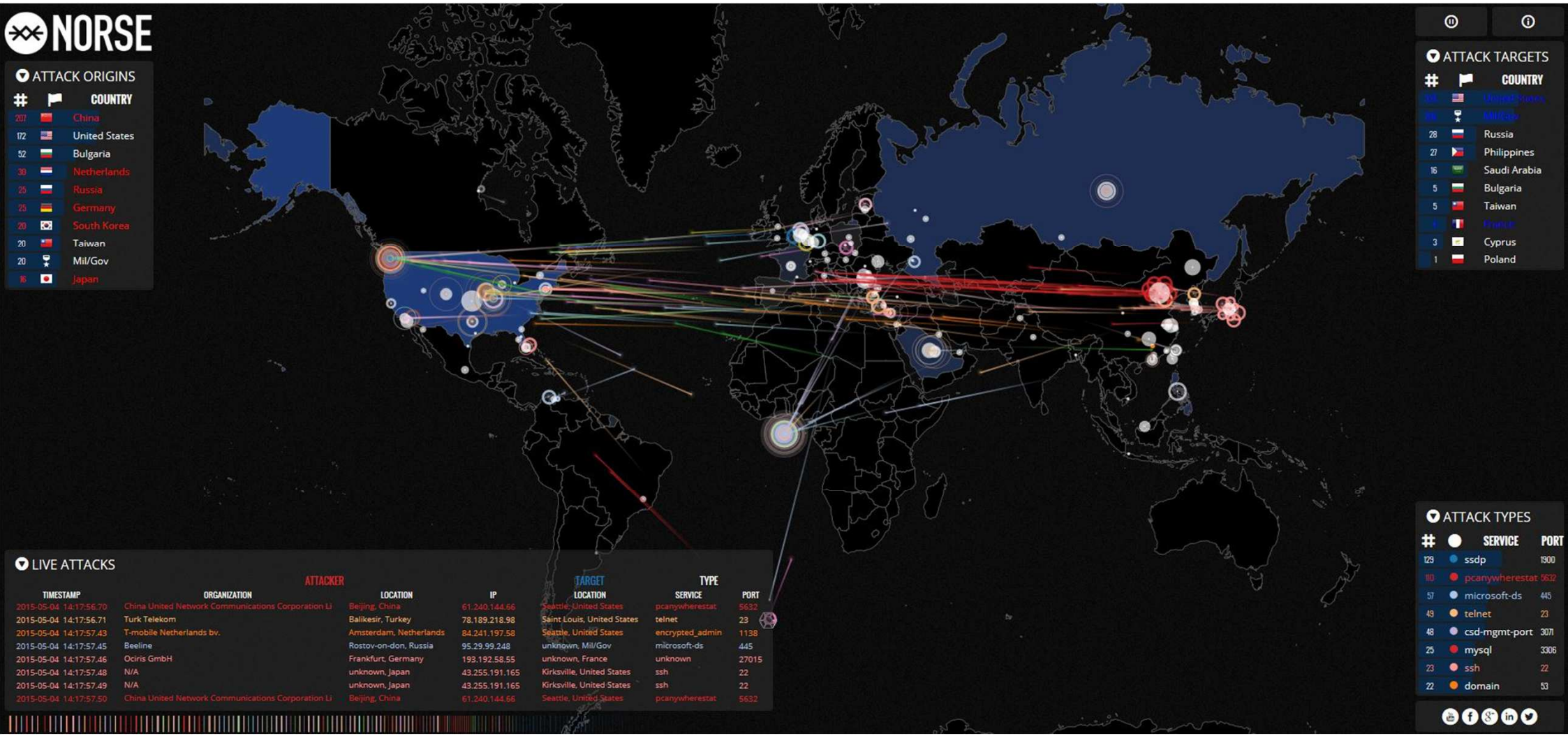
Denial of Service Attack

an attack on a computer or network that prevents legitimate use of its resources

What does it Affect?

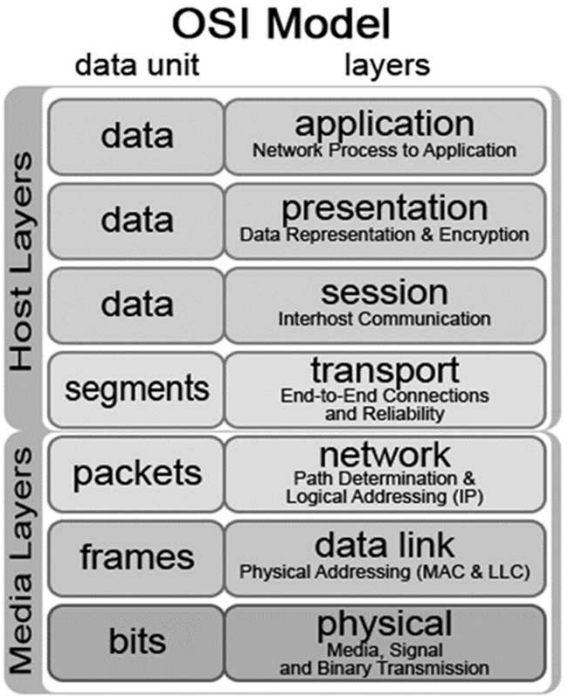
- Software Systems
- Network Equipment like Routers and Switches
- Servers and End-User PCs

Are there any attacks happening right now?


NORSE
ATTACK ORIGINS
COUNTRY
207 China
172 United States
52 Bulgaria
30 Netherlands
25 Russia
25 Germany
20 South Korea
20 Taiwan
20 Mil/Gov
16 Japan
ATTACK TARGETS
COUNTRY
28 Russia
27 Philippines
16 Saudi Arabia
5 Bulgaria
5 Taiwan
3 Cyprus
1 Poland
LIVE ATTACKS
ATTACKER
TARGET
TYPE
TIMESTAMP ORGANIZATION LOCATION IP LOCATION SERVICE PORT
2015-05-04 14:17:56.70 China United Network Communications Corporation Li Beijing, China 61.240.144.66 Seattle, United States pcanywherestat 5632
2015-05-04 14:17:56.71 Turk Telekom Balikesir, Turkey 78.189.218.98 Saint Louis, United States telnet 23
2015-05-04 14:17:57.43 T-mobile Netherlands bv. Amsterdam, Netherlands 84.241.197.58 Seattle, United States encrypted_admin 1138
2015-05-04 14:17:57.45 Beeline Rostov-on-don, Russia 95.29.99.248 unknown, Mil/Gov microsoft-ds 445
2015-05-04 14:17:57.46 Ociris GmbH Frankfurt, Germany 193.192.58.55 unknown, France unknown 27015
2015-05-04 14:17:57.48 N/A unknown, Japan 43.255.191.165 Kirksville, United States ssh 22
2015-05-04 14:17:57.49 N/A unknown, Japan 43.255.191.165 Kirksville, United States ssh 22
2015-05-04 14:17:57.50 China United Network Communications Corporation Li Beijing, China 61.240.144.66 Seattle, United States pcanywherestat 5632
ATTACK TYPES
SERVICE PORT
129 ssdp 1900
110 pcanywherestat 5632
57 microsoft-ds 445
49 telnet 23
48 csd-mgmt-port 3071
25 mysql 3306
23 ssh 22
22 domain 53

OSI Reference Model

The OSI Model is a always a good starting point to understand and troubleshoot network behaviour and this is especially true, when the network is under heavy stress like in the case of a DDoS Attack.



Analysis of an Attack

An attack can be conducted at any level of the OSI Layer:

OSI Layer	Example of Attacks
7	PDF GET requests, HTTP GET, HTTP POST, = website forms
6	Malformed SSL Requests -- Inspecting SSL encryption packets is resource intensive.
5	Telnet DDoS-attacker exploits Telnet server software running on switches and routers
4	SYN Flood, Smurf Attack
3	ICMP Flooding
2	MAC flooding -- inundates the network switch with data packets
1	Physical destruction, obstruction, manipulation, or malfunction of physical assets

DoS Shortfalls

DoS attacks are unable to attack large bandwidth websites – one upstream client cannot generate enough bandwidth to cripple major websites with a large bandwidth capability

What about **DDoS** Attacks?

Distributed Denial of Service Attacks (DDoS)

As described by Webopedia: **DDoS** is a type of **DoS** attack where multiple compromised systems (bot or zombie) -- which are usually infected with a Trojan -- are used to target a single system causing a Denial of Service (DoS) attack

DDoS can be of a very large scale potentially bringing down a whole network or an Internet Service Provider

How big?

Example of Real Life DDoS #1

Attacked Entity: Spamhouse

Date: 27th March 2013

Peak: 300 Gigabits per second

Type: DNS Reflection

Mitigation: Redirected Traffic to Cloudflare

MikroTik Devices with the DNS Server feature enabled, and left open to resolve names to the public, could have potentially been used during such an attack.

Reference: http://arstechnica.com/information-technology/2013/03/how-spamhaus-attackers-turned-dns-into-a-weapon-of-mass-destruction/

Example of Real Life DDoS #2

Attacked Entity: Cloudflare

Date: 10th February 2014

Peak: 400 gigabits per second

Type: NTP Reflection and Amplification

MikroTik Devices with NTP Server Service feature left open to resolve to the public could have potentially been used during such an attack.

Reference: http://arstechnica.com/security/2014/02/biggest-ddos-ever-aimed-at-cloudflares-content-delivery-network/

Are we at risk to such attacks?

A Botnet (also known as a zombie army) is a resource which is easily available to be used against us! These are infected computers located around the world which can be *rented* to launch such an attack.

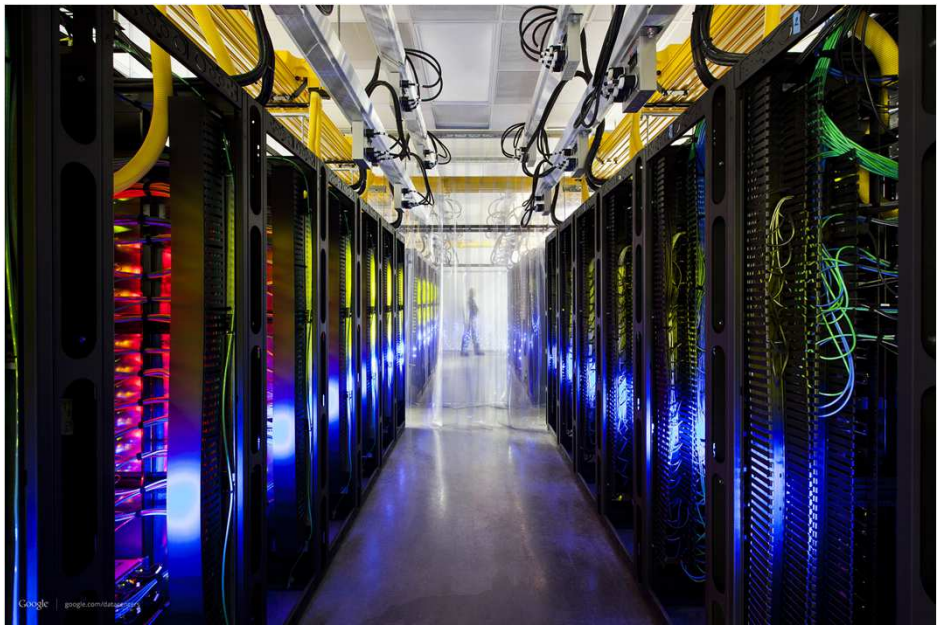
Just as an example, an online search returns the price to rent 1,000 infected computers in the United States for the costs of $180. If the hosts are located in the United Kingdom, the price is $240. France and Russia both costs $200, Canada costs $270, and 1,000 infected computers located around the world costs $35.

Mitigating a DoS/DDoS Attacks

Device	Layer	DoS Protections
Router	3-4	RP Filter, Routing Black Hole
Firewall	4-7	Address List, Session Limits, Syn Cookie

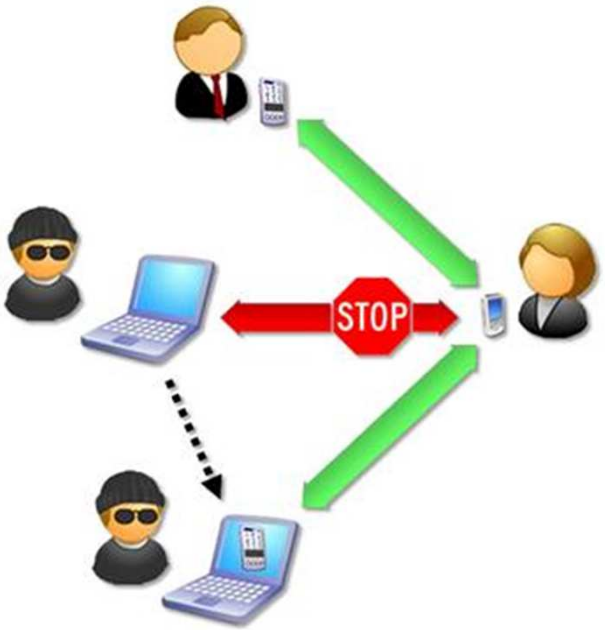
Tools to mitigate threats at router level

- rp_filter
- Routing Blackhole



Kind of attacks mitigated

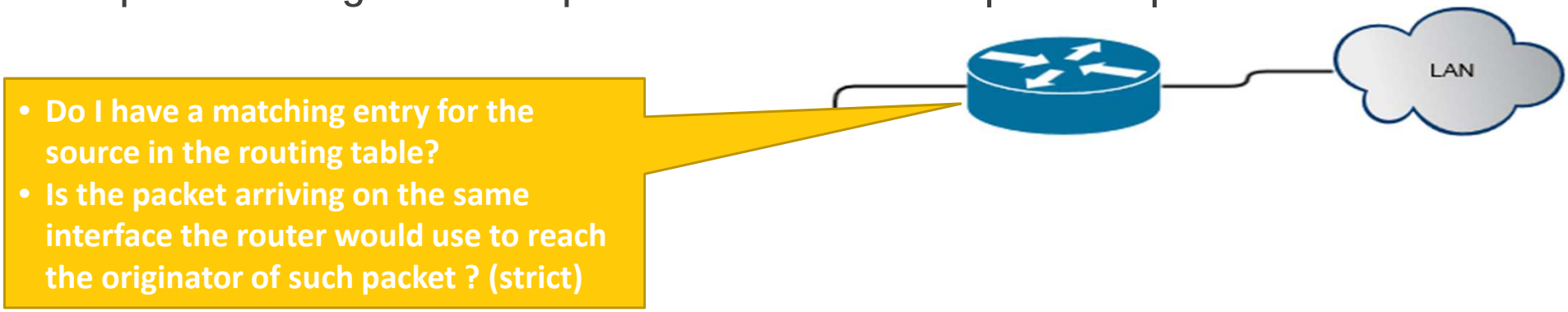
- Smurf Attacks
- IP address spoofing
- Malformed traceroute attack



Unicast Reverse Path Forwarding (RFC3704)

Used to stop spoof attacks on the outbound side.

- `/ip settings set rp-filter=strict|loose|no`



Underlying principle of rp_filter is to block outbound traffic if the IP does not belong to the subnet that resides on the LAN

Unicast Reverse Path Forwarding

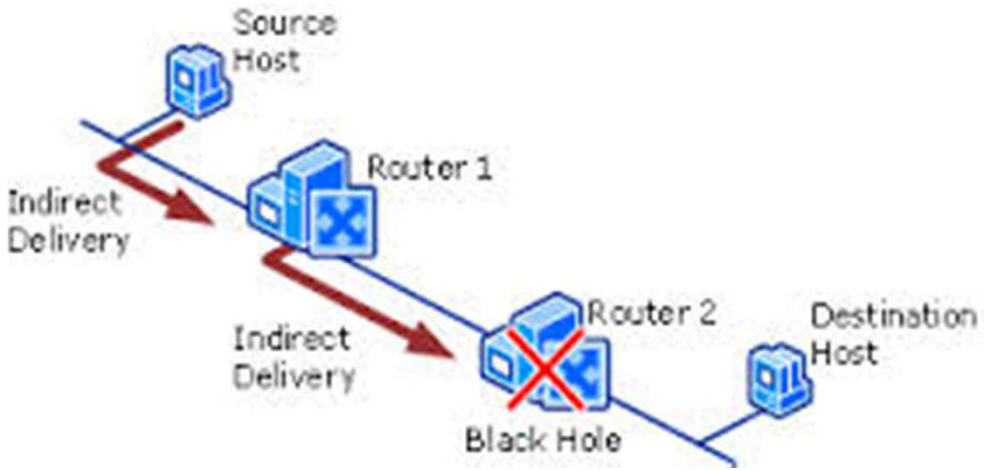
To be truly effective, rp_filter should be implemented in front of every potential source of attack

If asymmetric routing is taking place on border gateway, then only loose method can be used

Sometimes attackers can spoof source IP addresses from within the same autonomous system, making the strategy easily vulnerable

Routing Black Hole

The underlying idea is to black hole offending AS(s) from the local network so traffic is not routed from the border router to the LAN



The IP being targeted is no longer reachable but the rest of the network stays up

Routing Black Hole

Advantage:

- Our attacked IP range will appear dead to attackers since we would stop sending any replies back, making them thing that they have succeeded, while we can still exchange data with everyone else;

Disadvantage:

- Depending on the type of attack, lots of packets could be sent using spoofed source IP address. It could be the case that, if you also have servers with the same flaw in your network, you could amplify such an attack yourself towards the spoofed address, which in this case could be the victim (Reflection Attack);

Tools to mitigate threats at firewall level

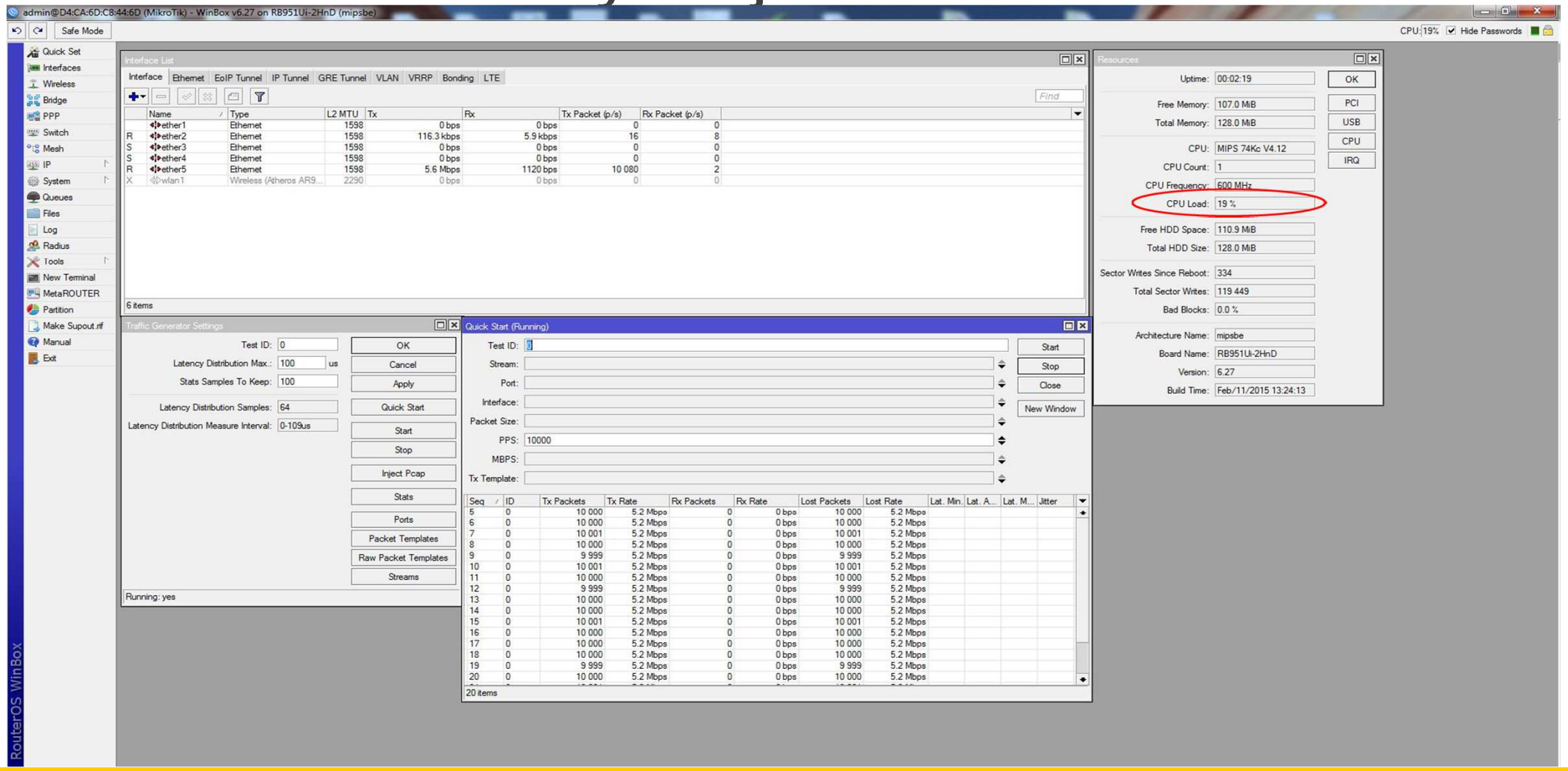
- Address Lists
- NAT (use with care)
- tcp_syncookies
- PSD
- Connections or Packets per second

Kind of attacks mitigated

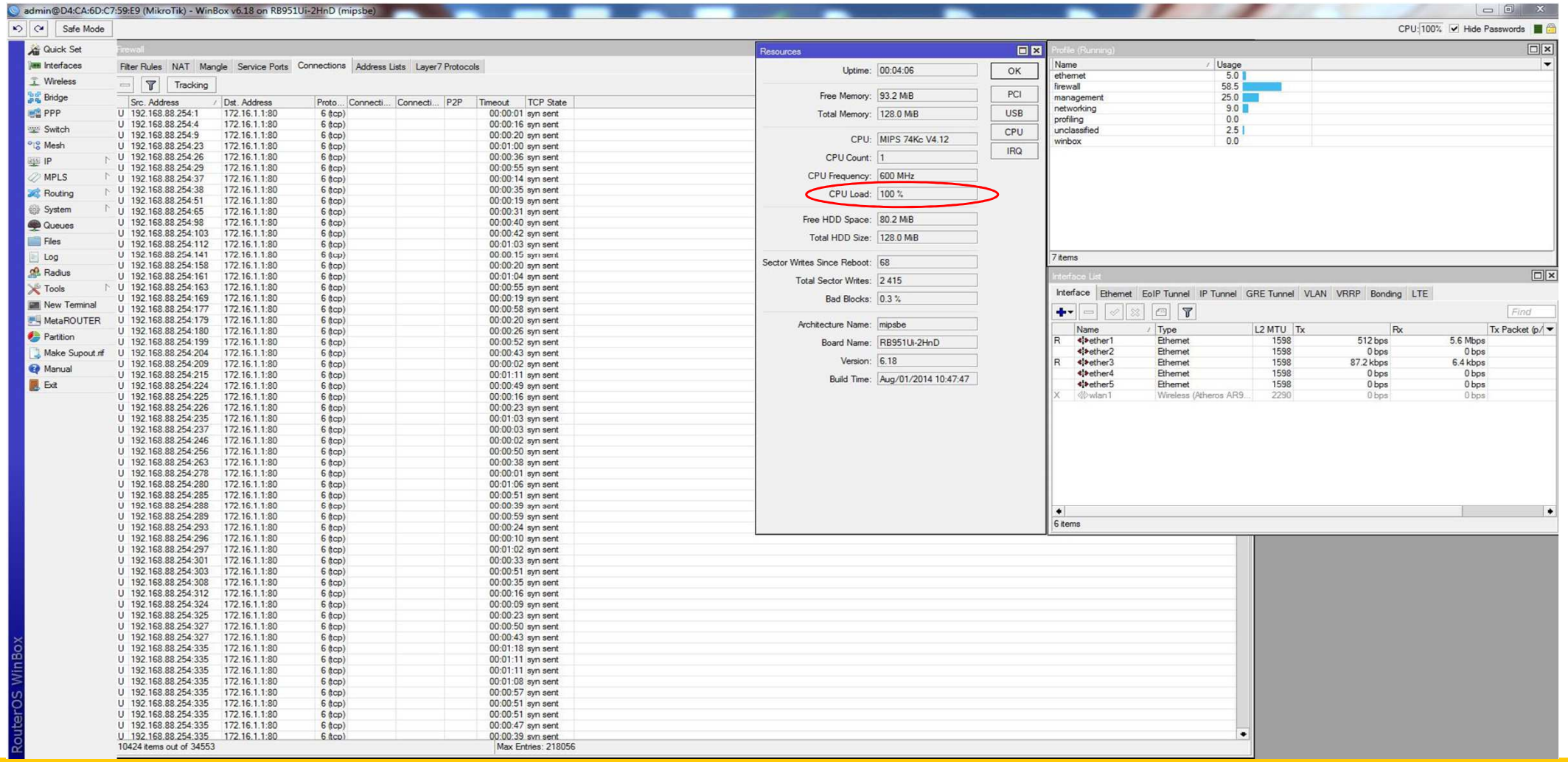
- SYN Floods
- SYN + ACK Attacks (3rd packet attacks)
- Reduce the impact of reflection attacks

We shall now demonstrate a simple SYN Attack!

Live Demo – Syn Injector Router



Live Demo – Target Router



Address Lists

Purpose

- Used to group blocks of IP addresses
- Entries can be added statically or dynamically by firewall rules

Requirement

- To identify host/networks exceeding our parameters and block them accordingly

TCP SynCookies

TCP SYN cookie is a technique used to resist SYN flood attacks by manipulating the sequence number in the TCP header

```
/ip settings tcp_syncookies yes | no
```

Even if it does NOT break any protocol specifications, restrictions on the tcp options will lead to a reduction in performance

It would be nice if could be enabled on port basis, but this a Linux Kernel Limitation

RouterOS Commands

```
/ip firewall mangle add action=add-src-to-address-
list address-list=suspicious address-list-timeout=5m
chain=prerouting dst-port=23 protocol=tcp
```

Matching conditions to create address-list

```
/ip firewall filter add action=log chain=input src-
address-list=suspicious
```

Action to be applied to the dynamic address-list

Attack Detection

We need to know if the system is under attack

```
/system resource cpu print
/system profile
/ip firewall filter print stats interval=3
/ip firewall connection print interval=3
```

Network Address Translation

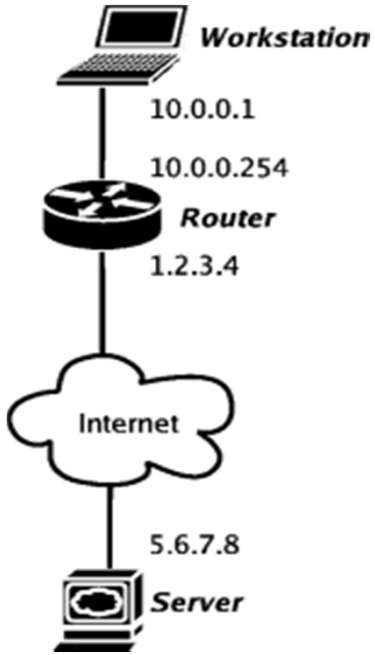
NAT enables translation of IP addresses used within one network to different IP addresses known within another network

Related RouterOS commands:

```
/ip firewall nat
```

Good Guys → Allow DST-NAT

Bad Guys → Do NOT DST-NAT



Network Address Translation

NAT is commonly accepted as a basic way to avoid DoS attacks

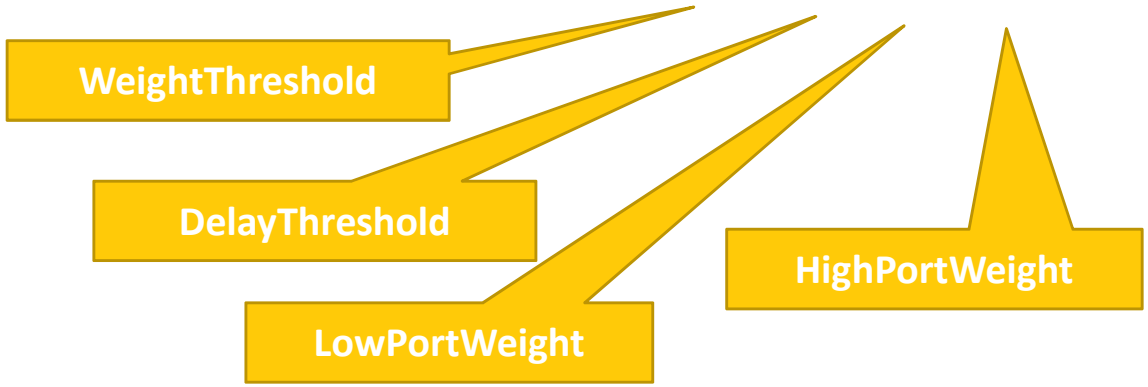
It does not really solve the problem… it moves it away stopping unsolicited inbound traffic from reaching the host on the LAN

Depending on the intensity of the attack NAT might turn against you because it will create a SINGLE bottleneck (NAT router itself)

Port Scan Detection

PSD is a firewall matcher included in RouterOS used to detect tcp and udp scans

```
/ip firewall mangle add chain=prerouting
protocol=tcp tcp-flags=syn psd=18,2s,3,1
```



Port Scan Detection

```
/ip firewall mangle add chain=prerouting protocol=tcp
tcp-flags=syn psd=18,2s,3,1
```

This means:

- A syn packet on a port lower than 1024, then PSD assigns a weight of 3
- A syn packet on a port higher than 1024, then PSD assigns a weight of 1
- PSD sums weights for packets that have been seen within 2 seconds from each other
- If a total of 18 has been reached than the rule matches

Port Scan Detection

It is not a true aid against DDoS attacks, but it can be useful to identify the offending networks

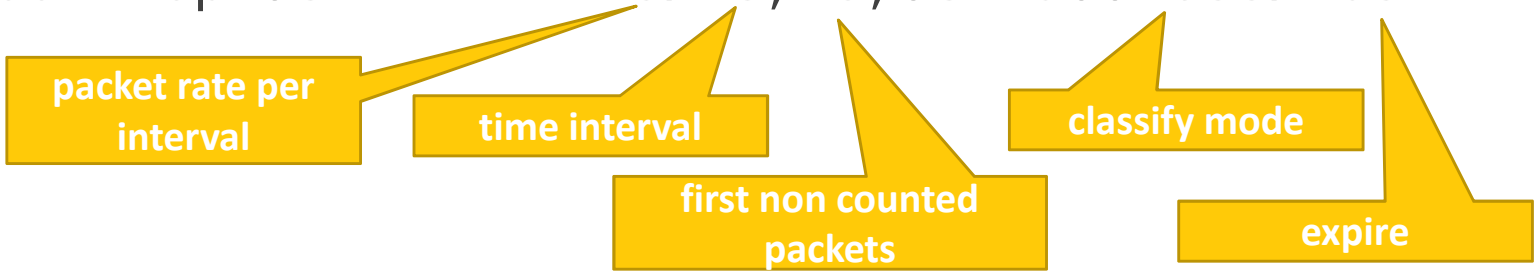
Can be used in combination with address-lists

Provided that connection tracking is already enabled, PSD does NOT have a high impact on resources, such as CPU

Connections / Packets per second

Best matcher to identify flows that exceed a given limit

```
/ip firewall filter chain=prerouting action=accept
protocol=tcp dst-limit=25/1s,25,dst-address/10s
```



Match packets until a given pps limit is exceeded for every destination IP address and destination port combination.

Putting all together

From the MikroTik wiki:

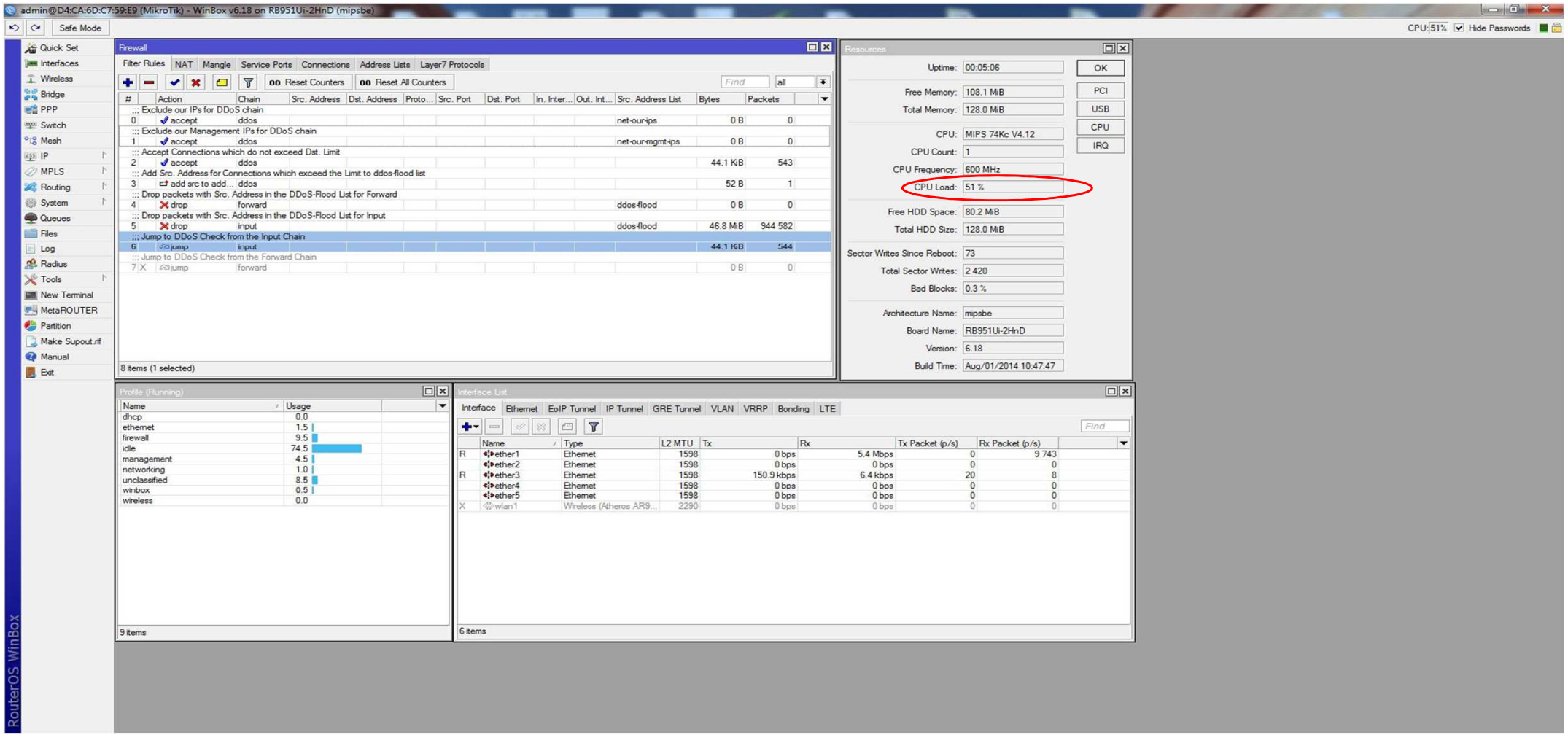
```
/ip firewall filter add chain=input protocol=tcp connection-limit=LIMIT,32  action=add-src-to-address-list  address-list=blocked-addr address-list-timeout=1d

/ip firewall filter add chain=input protocol=tcp src-address-list=blocked-addr connection-limit=3,32 action=tarpit

/ip firewall filter add chain=forward protocol=tcp tcp-flags=syn connection-state=new action=jump jump-target=SYN-Protect comment="SYN Flood protect" disabled=yes /ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn limit=400,5 connection-state=new action=accept comment="" disabled=no

/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn connection-state=new  action=drop comment="" disabled=no
```

Putting all together

What we use:

```
/ip firewall filter add chain=ddos comment="DDoS Protection" src-address-list=net-our-ips action=accept
/ip firewall filter add chain=ddos src-address-list=net-our-mgmt-ips action=accept
/ip firewall filter add chain=ddos dst-limit=25,25,src-and-dst-addresses/10s action=accept
/ip firewall filter add chain=ddos action=add-src-to-address-list address-list=ddos-flood address-list-timeout=30m
/ip firewall filter add chain=forward connection-state=new src-address-list=ddos-flood action=drop
```

Live Demo – After Mitigation



Fancy Solutions

DNS + NAT

- Change DNS response to point to a different NAT router

Remotely triggered Black Hole

- Inject null route into BGP to make all the routers of the AS drop the traffic for the offending prefix without having to elaborate with any access lists

A common BGP community that our upstream peer can Black Hole

- Requires upstream provider cooperation

Fancy Solutions

Bogon Feed

- Have an external source feed us with details of common threats originating prefixes on the internet, updated via BGP
- One for example is Team Cymru

Conclusions

DoS and DDoS Attacks can be conducted at any level

There are a few solution to mitigate a DDoS Attack at both the router level and the firewall level

However almost any service may be overloaded by a very large number of requests

Hardware plays an important part. A faster router, server or a bigger bandwidth channel will make a huge difference when trying to resist a DDoS Attack

References

- http://wiki.mikrotik.com
- https://www.us-cert.gov/
- http://www.arstechnica.com
- http://www.norse-corp.com

Thank You!

Questions and Suggestions

- Alfredo Giordano (alfredo@tiktrain.com)
- Matthew Ciantar (matthew@tiktrain.com)