

Reducing the impact of DoS attacks with MikroTik RouterOS

Alfredo Giordano
Matthew Ciantar



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?

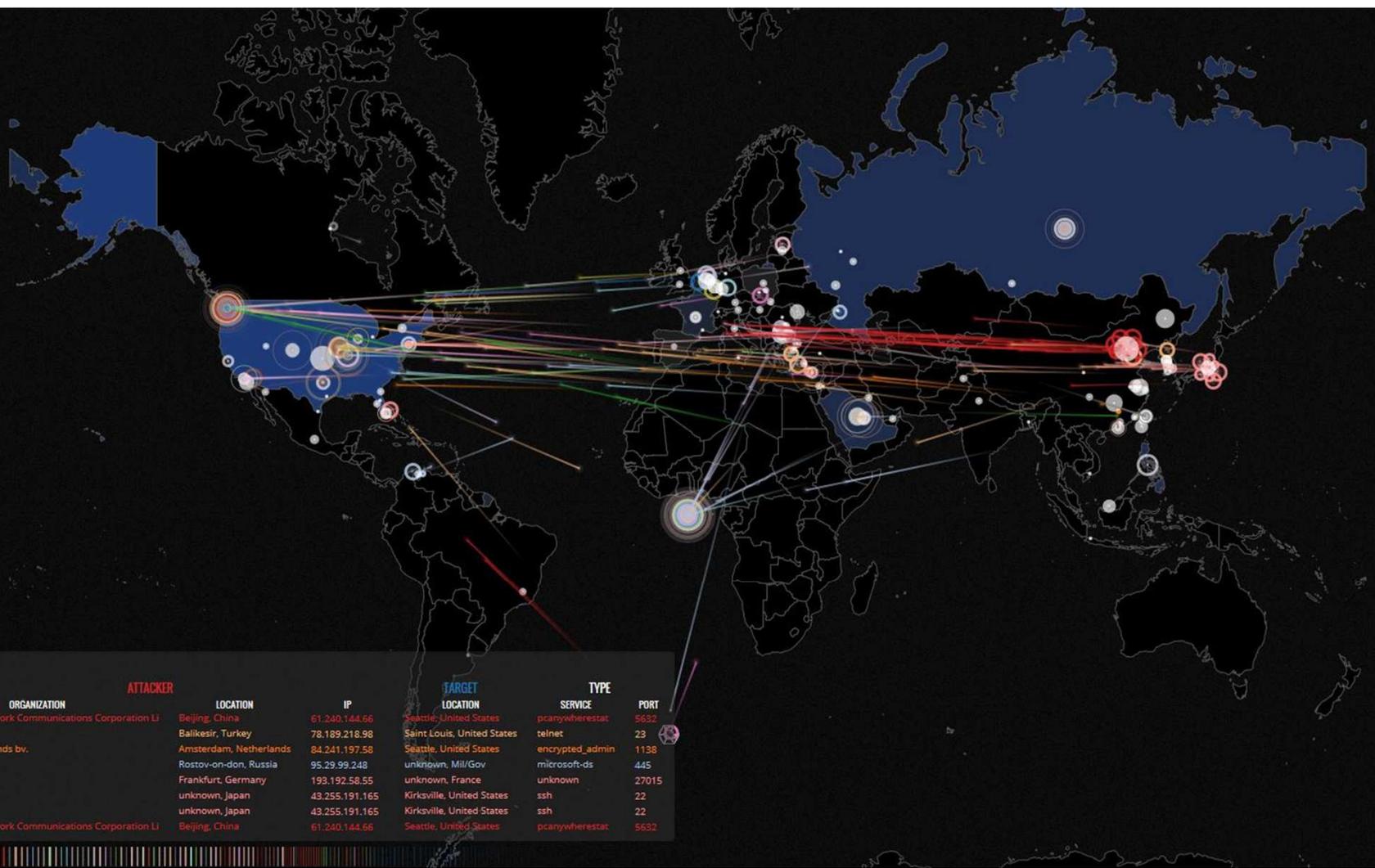
- Software Systems
- Network Equipment like Routers and Switches
- Servers and End-User PCs

Are there any attacks happening right now?



ATTACK ORIGINS

#	COUNTRY
207	China
172	United States
52	Bulgaria
30	Netherlands
26	Russia
25	Germany
20	South Korea
20	Taiwan
20	Mil/Gov
16	Japan



ATTACK TARGETS

#	COUNTRY
104	United States
84	Mil/Gov
28	Russia
27	Philippines
16	Saudi Arabia
5	Bulgaria
5	Taiwan
4	France
3	Cyprus
1	Poland

LIVE ATTACKS

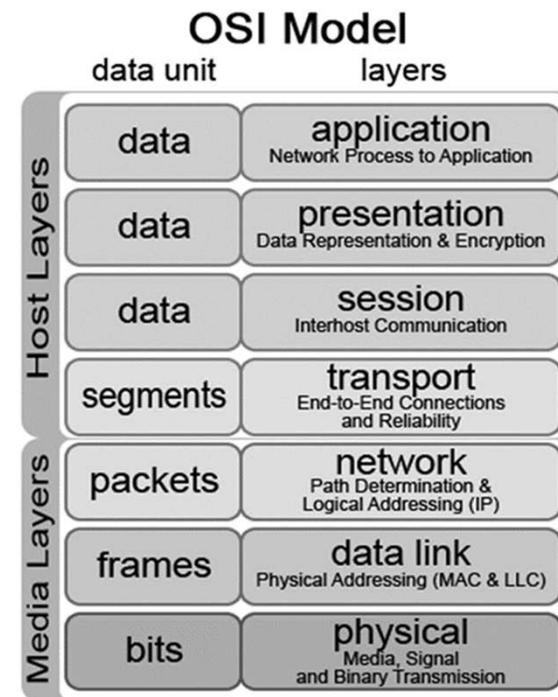
TIMESTAMP	ORGANIZATION	ATTACKER	LOCATION	IP	TARGET	LOCATION	SERVICE	TYPE	PORT
2015-05-04 14:17:56.70	China United Network Communications Corporation Li		Beijing, China	61.240.144.66	Seattle, United States		pcanywheresat		5632
2015-05-04 14:17:56.71	Turk Telekom		Balkesir, Turkey	78.189.218.98	Saint Louis, 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		pcanywheresat		5632

ATTACK TYPES

#	SERVICE	PORT
129	ssdp	1900
100	pcanywheresat	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 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 Wikipedia: **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

How Spamhaus' attackers turned DNS into a weapon of mass destruction

DNS amplification can clog the Internet's core—and there's no fix in sight.

by Sean Gallagher - Mar 28, 2013 7:30pm GMT

Share Tweet 54



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

Biggest DDoS ever aimed at Cloudflare's content delivery network

Network Time Protocol attack reached 400Gbps.

by Sean Gallagher - Feb 11, 2014 5:12pm GMT

Share Tweet 59



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.

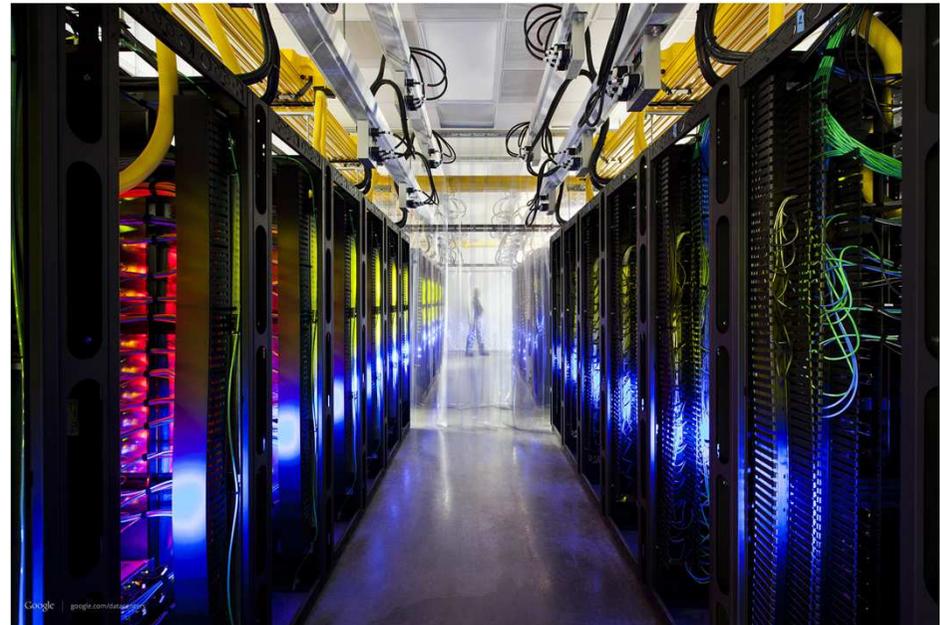
Just as an example, an online search returns the price to rent 1,000 infected computers in the United States for the costs of \$180. If the hosts are located in the United Kingdom, the price is \$240. France and Russia both costs \$200, Canada costs \$270, and 1,000 infected computers located around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

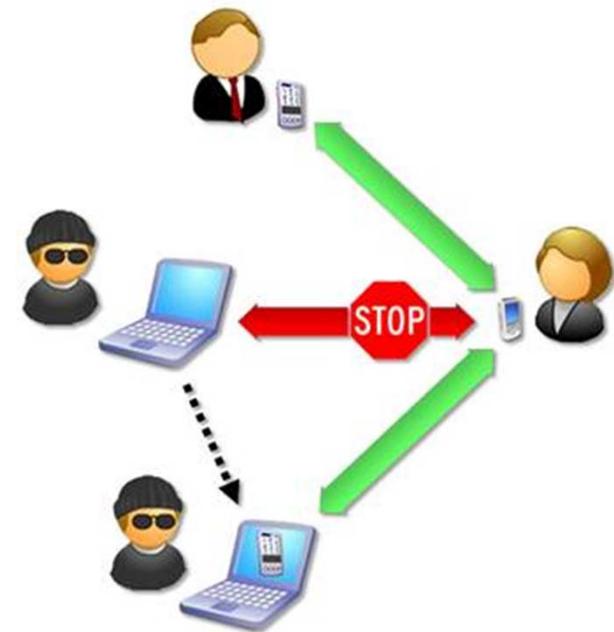
Tools to mitigate threats at router level

- rp_filter
- Routing Blackhole



Kind of attacks mitigated

- Smurf Attacks
- IP address spoofing
- Malformed traceroute attack

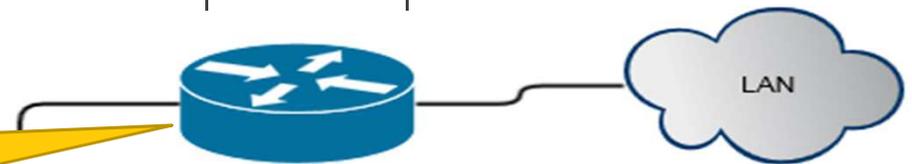


Unicast Reverse Path Forwarding (RFC3704)

Used to stop spoof attacks on the outbound side.

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

- Do I have a matching entry for the source in the routing table?
- Is the packet arriving on the same interface the router would use to reach the originator of such packet ? (strict)



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

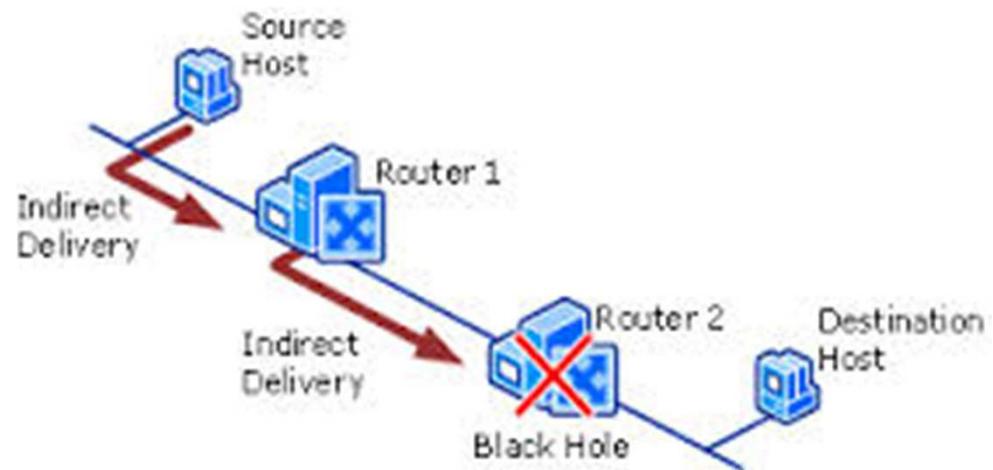
To be truly effective, rp_filter should be implemented in front of every potential source of attack

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 think 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

admin@D4:CA:6D:C8:44:6D (MikroTik) - WinBox v6.27 on RB951Ui-2HnD (mipsbe)

Safe Mode CPU:19% Hide Passwords

Interface List

Interface	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRPP	Bonding	LTE
Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)		
R ether1	Ethernet	1598	0 bps	0 bps	0	0		
R ether2	Ethernet	1598	116.3 kbps	5.9 kbps	16	8		
S ether3	Ethernet	1598	0 bps	0 bps	0	0		
S ether4	Ethernet	1598	0 bps	0 bps	0	0		
R ether5	Ethernet	1598	5.6 Mbps	1120 bps	10 080	2		
X wlan1	Wireless (Atheros AR9...	2250	0 bps	0 bps	0	0		

6 items

Traffic Generator Settings

Test ID: 0 OK Cancel

Latency Distribution Max.: 100 us Apply

Stats Samples To Keep: 100

Latency Distribution Samples: 64 Quick Start

Latency Distribution Measure Interval: 0-109us Start Stop

Inject Pcap

Stats

Ports

Packet Templates

Raw Packet Templates

Streams

Running: yes

Quick Start (Running)

Test ID: 1 Start Stop Close New Window

Stream: []

Port: []

Interface: []

Packet Size: []

PPS: 10000

MBPS: []

Tx Template: []

Seq / ID	Tx Packets	Tx Rate	Rx Packets	Rx Rate	Lost Packets	Lost Rate	Lat. Min.	Lat. A...	Lat. M...	Jitter
5 0	10 000	5.2 Mbps	0	0 bps	10 000	5.2 Mbps				
6 0	10 000	5.2 Mbps	0	0 bps	10 000	5.2 Mbps				
7 0	10 001	5.2 Mbps	0	0 bps	10 001	5.2 Mbps				
8 0	10 000	5.2 Mbps	0	0 bps	10 000	5.2 Mbps				
9 0	9 999	5.2 Mbps	0	0 bps	9 999	5.2 Mbps				
10 0	10 001	5.2 Mbps	0	0 bps	10 001	5.2 Mbps				
11 0	10 000	5.2 Mbps	0	0 bps	10 000	5.2 Mbps				
12 0	9 999	5.2 Mbps	0	0 bps	9 999	5.2 Mbps				
13 0	10 000	5.2 Mbps	0	0 bps	10 000	5.2 Mbps				
14 0	10 000	5.2 Mbps	0	0 bps	10 000	5.2 Mbps				
15 0	10 001	5.2 Mbps	0	0 bps	10 001	5.2 Mbps				
16 0	10 000	5.2 Mbps	0	0 bps	10 000	5.2 Mbps				
17 0	10 000	5.2 Mbps	0	0 bps	10 000	5.2 Mbps				
18 0	10 000	5.2 Mbps	0	0 bps	10 000	5.2 Mbps				
19 0	9 999	5.2 Mbps	0	0 bps	9 999	5.2 Mbps				
20 0	10 000	5.2 Mbps	0	0 bps	10 000	5.2 Mbps				

20 items

Resources

Uptime: 00:02:19 OK

Free Memory: 107.0 MB PCI

Total Memory: 128.0 MB USB

CPU: MIPS 74Kc V4.12 CPU

CPU Count: 1 IRQ

CPU Frequency: 600 MHz

CPU Load: 19 %

Free HDD Space: 110.9 MB

Total HDD Size: 128.0 MB

Sector Writes Since Reboot: 334

Total Sector Writes: 119 449

Bad Blocks: 0.0 %

Architecture Name: mipsbe

Board Name: RB951Ui-2HnD

Version: 6.27

Build Time: Feb/11/2015 13:24:13

Live Demo – Target Router

admin@D4:CA:6D:C7:59:E9 (MikroTik) - WinBox v6.18 on RB951Ui-2HnD (mipsbe)

Safe Mode CPU:100% Hide Passwords

Quick Set Firewall

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

Wireless Tracking

	Src. Address	Dst. Address	Proto...	Connecti...	Connecti...	P2P	Timeout	TCP State
U	192.168.88.254:1	172.16.1.1:80	6 tcp				00:00:01	syn sent
U	192.168.88.254:4	172.16.1.1:80	6 tcp				00:00:16	syn sent
U	192.168.88.254:9	172.16.1.1:80	6 tcp				00:00:20	syn sent
U	192.168.88.254:23	172.16.1.1:80	6 tcp				00:01:00	syn sent
U	192.168.88.254:26	172.16.1.1:80	6 tcp				00:00:36	syn sent
U	192.168.88.254:29	172.16.1.1:80	6 tcp				00:00:55	syn sent
U	192.168.88.254:37	172.16.1.1:80	6 tcp				00:00:14	syn sent
U	192.168.88.254:38	172.16.1.1:80	6 tcp				00:00:35	syn sent
U	192.168.88.254:51	172.16.1.1:80	6 tcp				00:00:19	syn sent
U	192.168.88.254:65	172.16.1.1:80	6 tcp				00:00:31	syn sent
U	192.168.88.254:98	172.16.1.1:80	6 tcp				00:00:40	syn sent
U	192.168.88.254:103	172.16.1.1:80	6 tcp				00:00:42	syn sent
U	192.168.88.254:112	172.16.1.1:80	6 tcp				00:01:03	syn sent
U	192.168.88.254:141	172.16.1.1:80	6 tcp				00:00:15	syn sent
U	192.168.88.254:158	172.16.1.1:80	6 tcp				00:00:20	syn sent
U	192.168.88.254:161	172.16.1.1:80	6 tcp				00:01:04	syn sent
U	192.168.88.254:163	172.16.1.1:80	6 tcp				00:00:55	syn sent
U	192.168.88.254:169	172.16.1.1:80	6 tcp				00:00:19	syn sent
U	192.168.88.254:177	172.16.1.1:80	6 tcp				00:00:58	syn sent
U	192.168.88.254:179	172.16.1.1:80	6 tcp				00:00:20	syn sent
U	192.168.88.254:180	172.16.1.1:80	6 tcp				00:00:26	syn sent
U	192.168.88.254:199	172.16.1.1:80	6 tcp				00:00:52	syn sent
U	192.168.88.254:204	172.16.1.1:80	6 tcp				00:00:43	syn sent
U	192.168.88.254:209	172.16.1.1:80	6 tcp				00:00:02	syn sent
U	192.168.88.254:215	172.16.1.1:80	6 tcp				00:01:11	syn sent
U	192.168.88.254:224	172.16.1.1:80	6 tcp				00:00:49	syn sent
U	192.168.88.254:225	172.16.1.1:80	6 tcp				00:00:16	syn sent
U	192.168.88.254:226	172.16.1.1:80	6 tcp				00:00:23	syn sent
U	192.168.88.254:235	172.16.1.1:80	6 tcp				00:01:03	syn sent
U	192.168.88.254:237	172.16.1.1:80	6 tcp				00:00:03	syn sent
U	192.168.88.254:246	172.16.1.1:80	6 tcp				00:00:02	syn sent
U	192.168.88.254:256	172.16.1.1:80	6 tcp				00:00:50	syn sent
U	192.168.88.254:263	172.16.1.1:80	6 tcp				00:00:38	syn sent
U	192.168.88.254:278	172.16.1.1:80	6 tcp				00:00:01	syn sent
U	192.168.88.254:280	172.16.1.1:80	6 tcp				00:01:06	syn sent
U	192.168.88.254:285	172.16.1.1:80	6 tcp				00:00:51	syn sent
U	192.168.88.254:288	172.16.1.1:80	6 tcp				00:00:39	syn sent
U	192.168.88.254:289	172.16.1.1:80	6 tcp				00:00:59	syn sent
U	192.168.88.254:293	172.16.1.1:80	6 tcp				00:00:24	syn sent
U	192.168.88.254:296	172.16.1.1:80	6 tcp				00:00:10	syn sent
U	192.168.88.254:297	172.16.1.1:80	6 tcp				00:01:02	syn sent
U	192.168.88.254:301	172.16.1.1:80	6 tcp				00:00:33	syn sent
U	192.168.88.254:303	172.16.1.1:80	6 tcp				00:00:51	syn sent
U	192.168.88.254:308	172.16.1.1:80	6 tcp				00:00:35	syn sent
U	192.168.88.254:312	172.16.1.1:80	6 tcp				00:00:16	syn sent
U	192.168.88.254:324	172.16.1.1:80	6 tcp				00:00:09	syn sent
U	192.168.88.254:325	172.16.1.1:80	6 tcp				00:00:23	syn sent
U	192.168.88.254:327	172.16.1.1:80	6 tcp				00:00:50	syn sent
U	192.168.88.254:327	172.16.1.1:80	6 tcp				00:00:43	syn sent
U	192.168.88.254:335	172.16.1.1:80	6 tcp				00:01:18	syn sent
U	192.168.88.254:335	172.16.1.1:80	6 tcp				00:01:11	syn sent
U	192.168.88.254:335	172.16.1.1:80	6 tcp				00:01:11	syn sent
U	192.168.88.254:335	172.16.1.1:80	6 tcp				00:01:08	syn sent
U	192.168.88.254:335	172.16.1.1:80	6 tcp				00:00:57	syn sent
U	192.168.88.254:335	172.16.1.1:80	6 tcp				00:00:51	syn sent
U	192.168.88.254:335	172.16.1.1:80	6 tcp				00:00:51	syn sent
U	192.168.88.254:335	172.16.1.1:80	6 tcp				00:00:47	syn sent
U	192.168.88.254:335	172.16.1.1:80	6 tcp				00:00:39	syn sent

10244 items out of 34553 Max Entries: 218056

Resources

Uptime: 00:04:06 OK

Free Memory: 93.2 MiB PCI

Total Memory: 128.0 MB USB

CPU: MIPS 74Kc V4.12 CPU

CPU Count: 1 IRQ

CPU Frequency: 600 MHz

CPU Load: 100 %

Free HDD Space: 80.2 MB

Total HDD Size: 128.0 MB

Sector Writes Since Reboot: 68

Total Sector Writes: 2 415

Bad Blocks: 0.3 %

Architecture Name: mipsbe

Board Name: RB951Ui-2HnD

Version: 6.18

Build Time: Aug/01/2014 10:47:47

Profile (Running)

Name	Usage
ethernet	5.0
firewall	58.5
management	25.0
networking	9.0
profiling	0.0
unclassified	2.5
winbox	0.0

7 items

Interface List

Interface	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE
R	ether1	Ethernet	1598	512 bps	5.6 Mbps			
R	ether2	Ethernet	1598	0 bps	0 bps			
R	ether3	Ethernet	1598	87.2 kbps	6.4 kbps			
R	ether4	Ethernet	1598	0 bps	0 bps			
R	ether5	Ethernet	1598	0 bps	0 bps			
X	wlan1	Wireless (Atheros AR9...	2290	0 bps	0 bps			

6 items

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

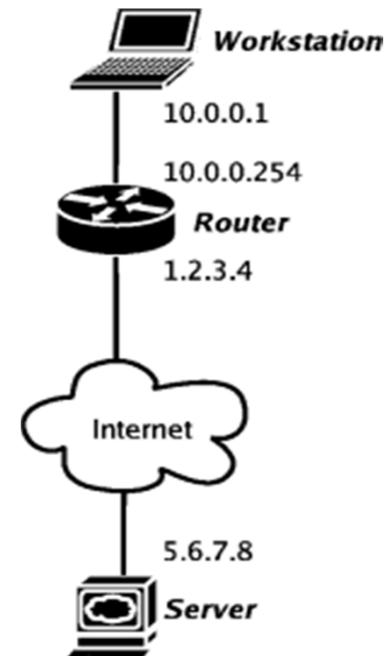
NAT enables translation of IP addresses used within one network to different IP addresses known within another network

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

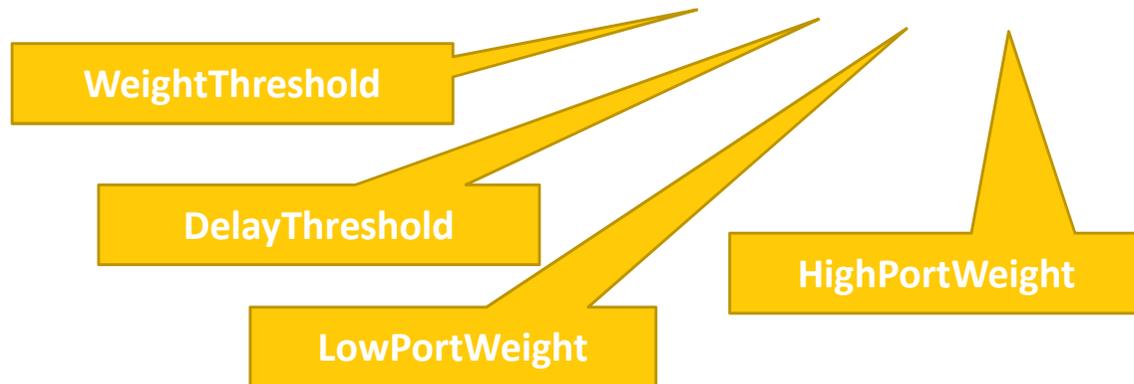
It does not really solve the problem... it moves it away stopping unsolicited inbound traffic from reaching the host on the LAN

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 then 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

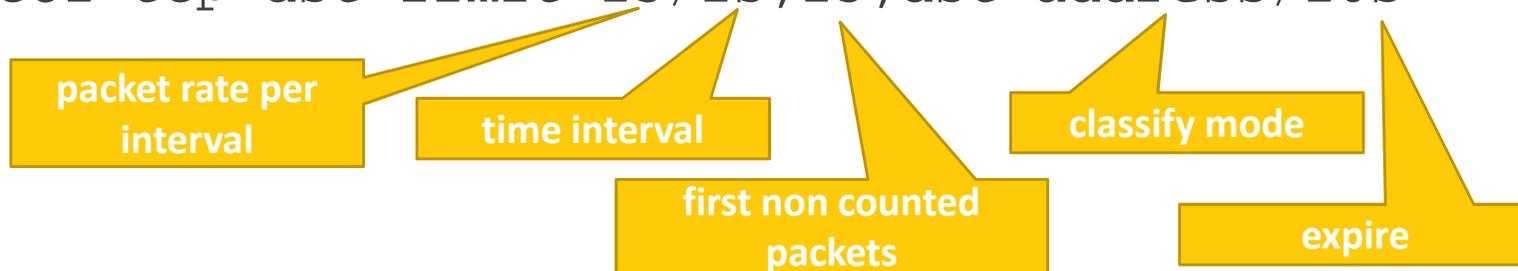
Can be used in combination with address-lists

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

admin@D4:CA:6D:C7:59:E9 (MikroTik) - WinBox v6.18 on RB951Ui-2HnD (mipsbe)

Safe Mode

CPU:51% Hide Passwords

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

00 Reset Counters 00 Reset All Counters

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Src. Address List	Bytes	Packets
0	accept	ddos								net-our-ips	0 B	0
1	accept	ddos								net-our-mgmt-ips	0 B	0
2	accept	ddos									44.1 KB	543
3	drop	ddos									52 B	1
4	drop	forward								ddos-flood	0 B	0
5	drop	input								ddos-flood	46.8 MB	944 582
6	jump	input									44.1 KB	544
7	jump	forward									0 B	0

8 items (1 selected)

Resources

Uptime: 00:05:06

Free Memory: 108.1 MB

Total Memory: 128.0 MB

CPU: MIPS 74Kc V4.12

CPU Count: 1

CPU Frequency: 600 MHz

CPU Load: 51 %

Free HDD Space: 80.2 MB

Total HDD Size: 128.0 MB

Sector Writes Since Reboot: 73

Total Sector Writes: 2 420

Bad Blocks: 0.3 %

Architecture Name: mipsbe

Board Name: RB951Ui-2HnD

Version: 6.18

Build Time: Aug/01/2014 10:47:47

Profile (Running)

Name	Usage
dhcp	0.0
ethernet	1.5
firewall	9.5
idle	74.5
management	4.5
networking	1.0
unclassified	8.5
winbox	0.5
wireless	0.0

9 items

Interface List

Interface	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE
R	ether1	Ethernet						
R	ether2	Ethernet						
R	ether3	Ethernet						
R	ether4	Ethernet						
R	ether5	Ethernet						
X	wlan1	Wireless (Atheros AR9...						

6 items

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)

