



Multi-stage DDoS filtering with Wanguard and more

PLONG 21, Kraków 1-2.10.2018 r.

www.itoro.com.pl

About ITORO



- **Wanguard implementations**
(**protection against DDoS attacks**)

- The only one
- Huge experience



- Tuning of servers and Linux systems
- We are helping to optimize costs
- Training on Wanguard systems



- Full support before and after installation
- Comprehensive service and advice
- Support for IT dept for smooth integration of Wanguard

Methods of collecting network traffic

- Port mirror
- Active / Passive monitoring
- sFLOW
- Packet Sampling
- NetFlow

What should be considered when choosing the best method:

- Network infrastructure
- Available protocols on routers
- Limits on the performance of routers and software

Why we are under attack ?

- Competition 😊
- Online Gaming
- Preparation for another attack (except DDoS)
- Fun with new botnet
- Extortion / blackmail
- Revenge for DDoS from Your network



Who is the target of DDoS attacks?

Data centers (hosting)

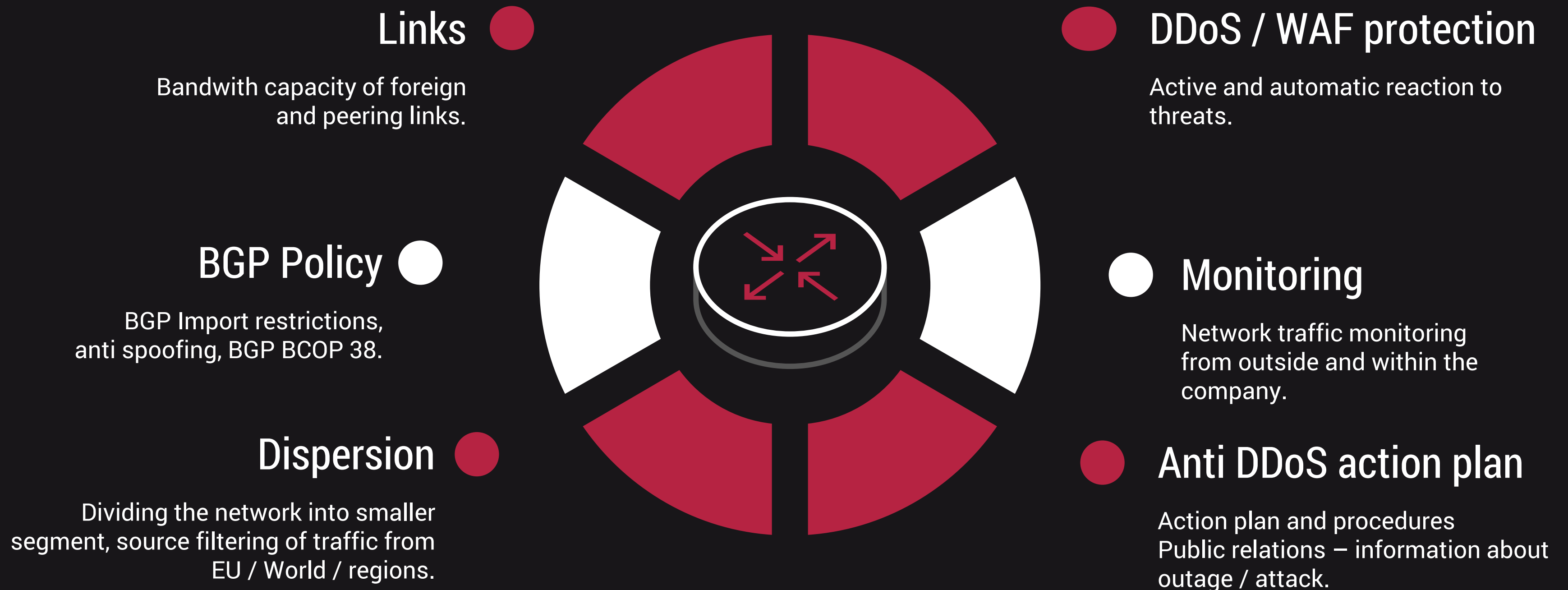
Internet Service Providers (ISP)

Government and financial institutions

Gambling and online gaming

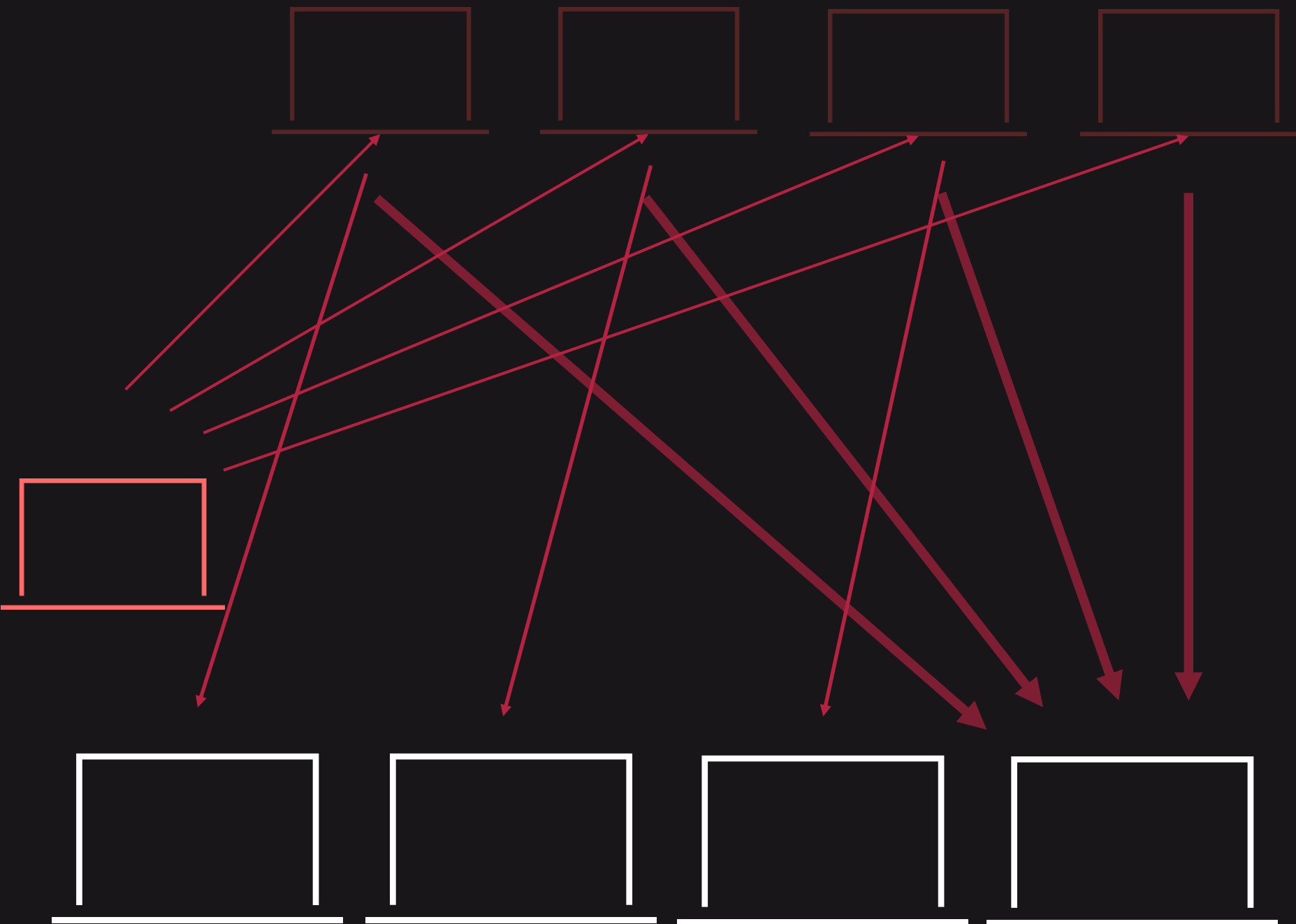


Good practices



Services that use amplification

Amplification	Protocol	Port
10000-51000	Memcached	11211
557	NTP	123
358	CharGEN	19
140	QOTD	17
28-54	DNS	53
56-70	C-LDAP	389
30	SSDP	1900
7-28	Portmap	111
6	SNMP	161
4	NetBIOS	137,138,139



Statistics – should I be scared?

SSDP
(UDP/1900)

Country	Total
China	754,310
Russian Federation	478,475
Korea, Republic of	317,018
Venezuela	194,793
United States	169,473



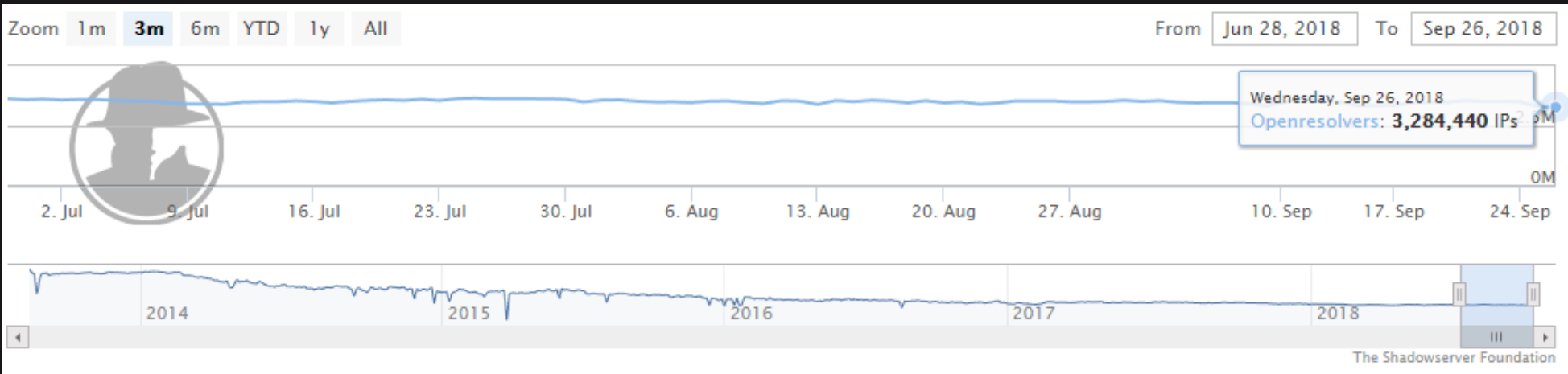
NTP
(UDP/123)

Country	Total
United States	738,940
Russian Federation	344,357
China	221,828
Brazil	158,221
Germany	139,066

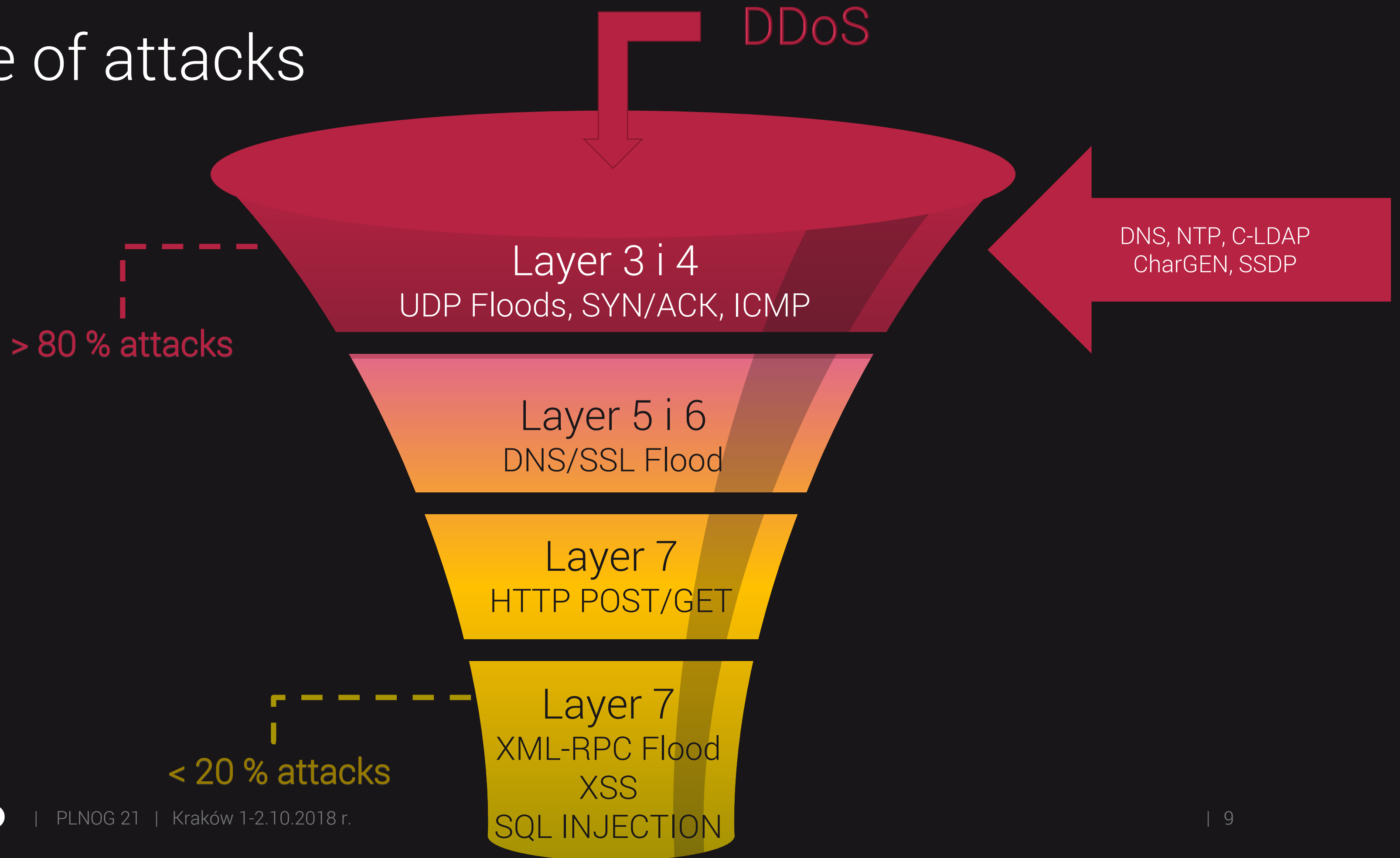


DNS
(UDP/53)

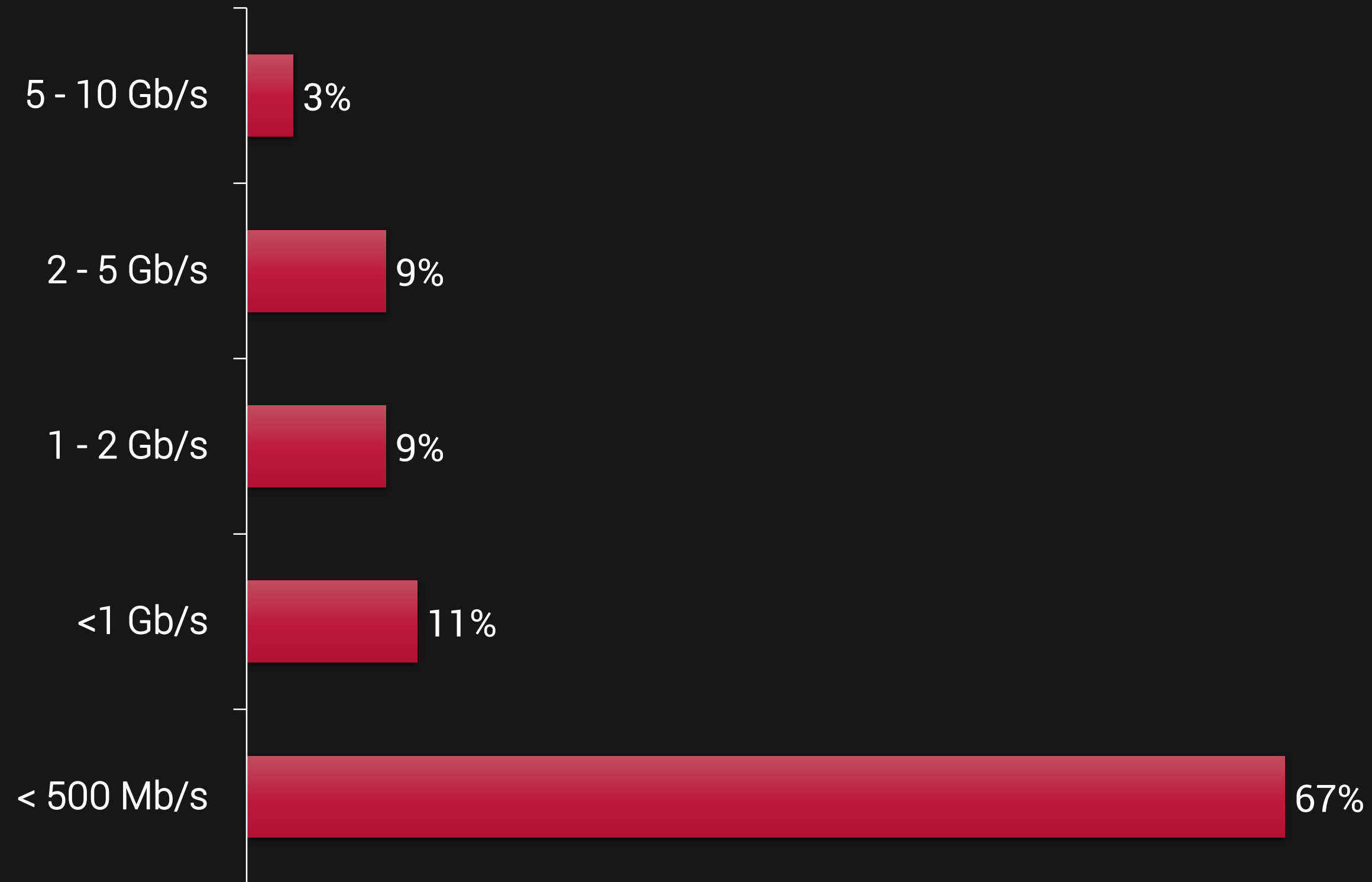
Country	Total
China	1,263,833
United States	319,053
Korea, Republic of	164,772
Russian Federation	144,922
Taiwan	115,780



Share of attacks



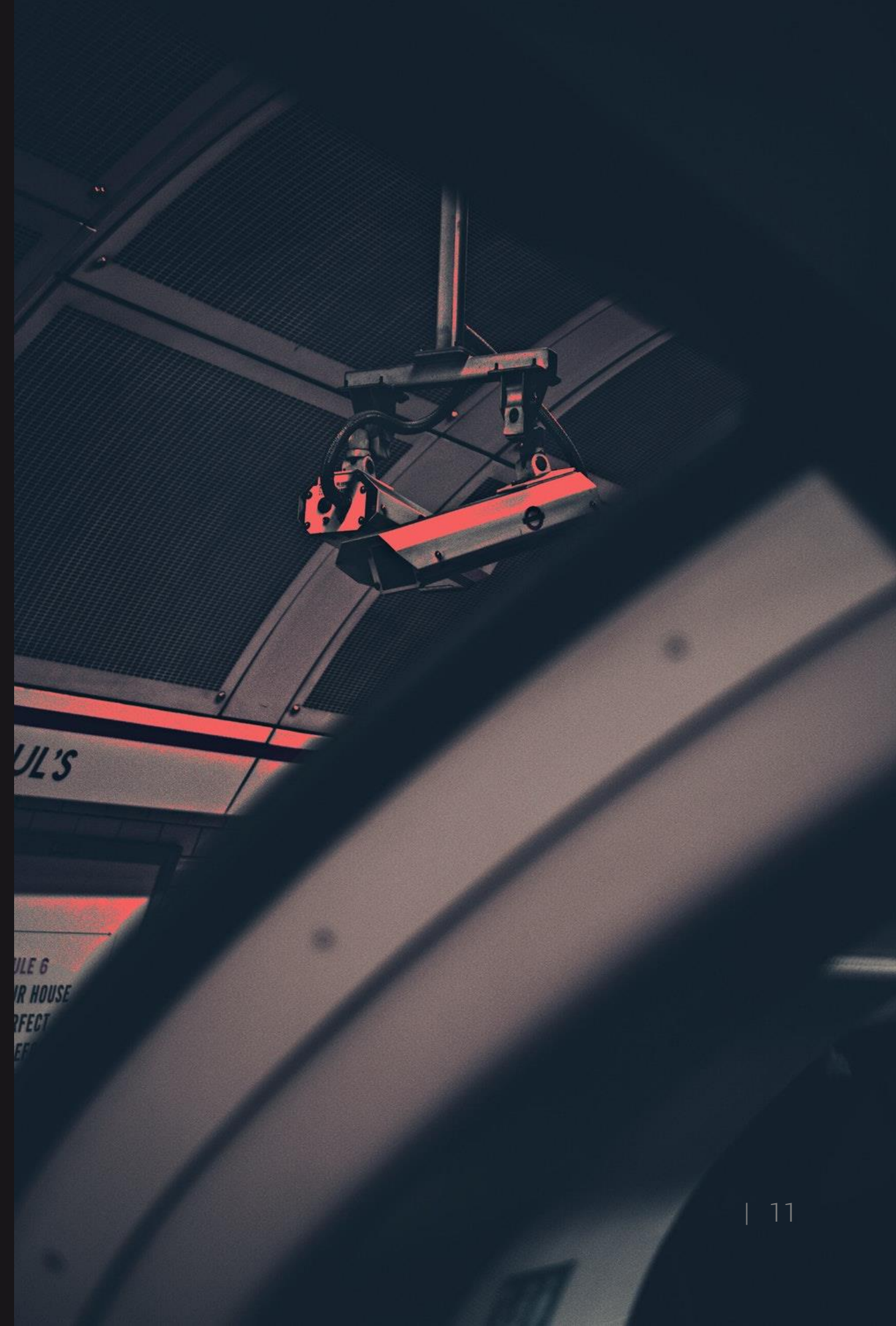
Attack speeds



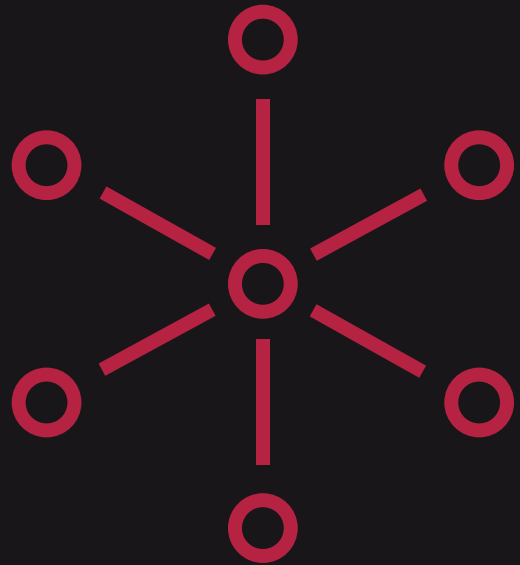
Summary for ISP

Comments

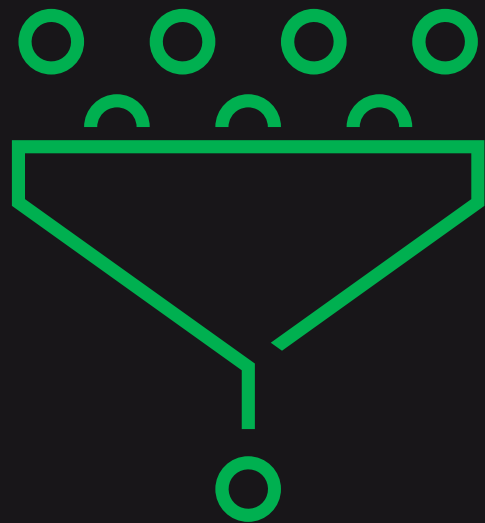
- ✓ Duration of attacks <30 seconds on subscribers
- ✓ Time of attacks on infrastructure – longer : 1-6 hours
- ✓ Multiple attack vectors (NTP / DNS / SSDP / ICMP)
- ✓ RTBH less effective –due to Carpet Bomb attacks



Important terms



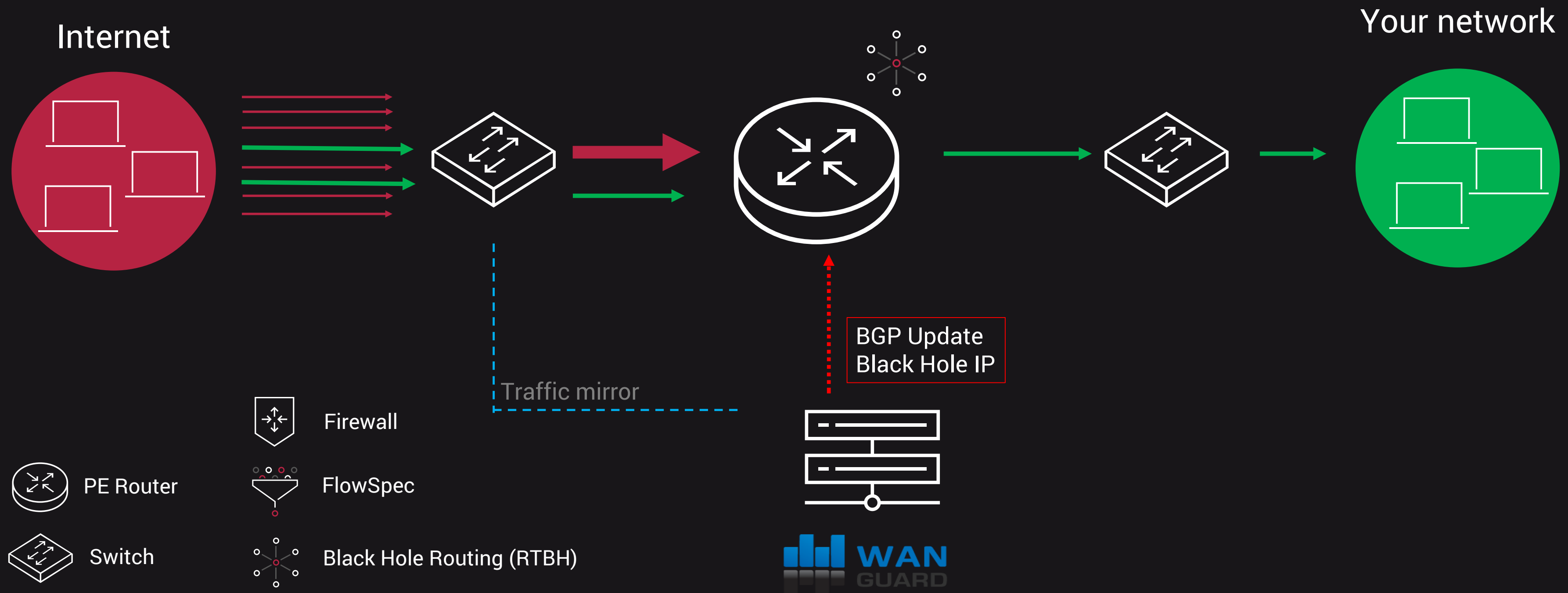
Black Hole Routing (Remotely Triggered Black Hole Routing)
The incoming traffic is discarded before entering Your network.



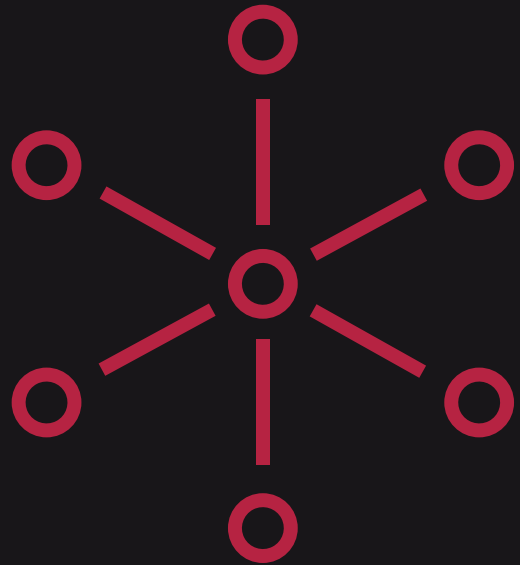
FlowSpec (RFC 5575)
Firewall filter rules are injected into BGP protocol.
Allows for different actions :

- drop / limit packets
- redirect
- setting of DSCP (Differentiated Services) used in QoS

Black Hole Routing

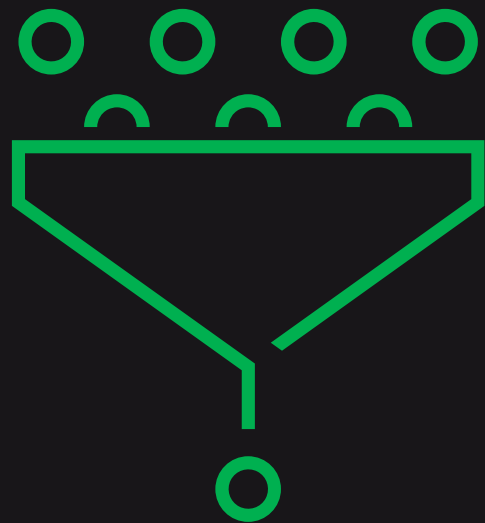


Possibilities of protection against DDoS attacks



Block traffic using **Remote Triggered Black Hole Routing (RTBH)**

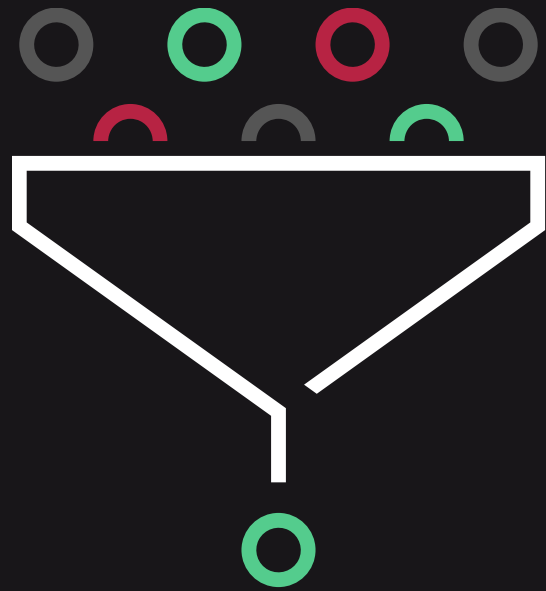
- Black Hole of IP / Network class
- Selective Black Hole routing (World / Regions / Country / Peering)



Filtering Traffic:

- Blocking or limiting protocols that use amplifications
- Filtering on servers using network cards (hardware) or iptables
- Filtering using FlowSpec on routers

FlowSpec



FlowSpec rules :

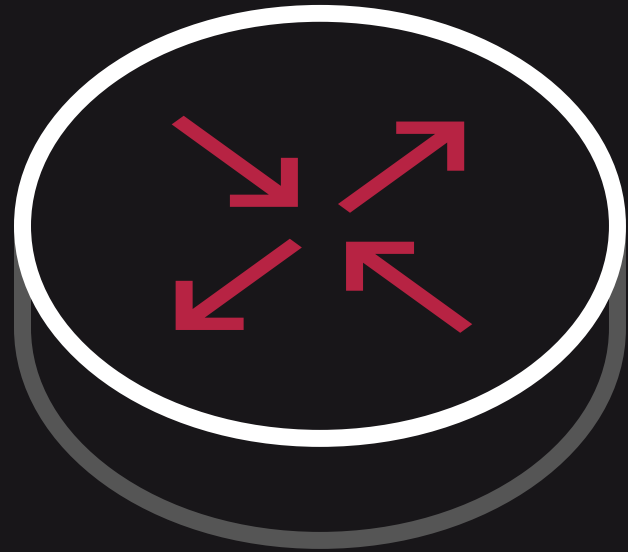
- Source / Destination IP
- Source / Destination Port
- Protocol
- Packet length
- TCP flags
- IP fragmentation



FlowSpec actions:

- Traffic limits (example: 10 Mb/s or 0)
- Traffic marking - DSCP
- Redirect - Target VRF (Juniper & Cisco)
- Redirect - IP NextHop (Cisco)

FlowSpec



CISCO – Limit 3000 rules

ASR 1xxx

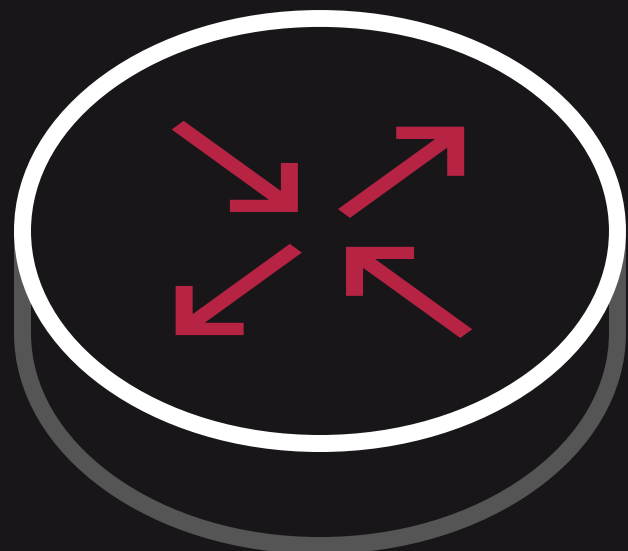
ASR 9xxx

CSR 1000v

CRS-3 (Taiko) LC, CRS-X (Topaz) LC

NCS 5500/6000

XRv 9000



Juniper – Limit 8000 rules

MX series

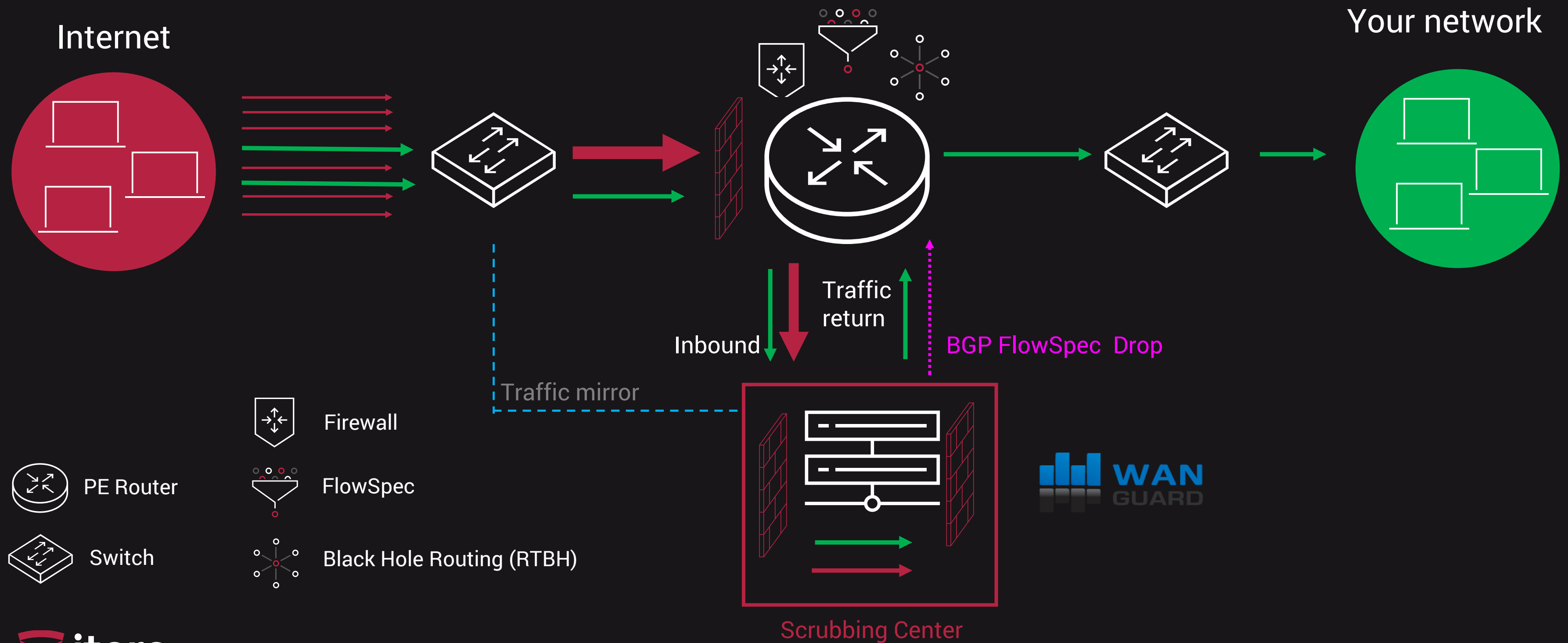
PTX 10002

QFX 1000[2/8/16]

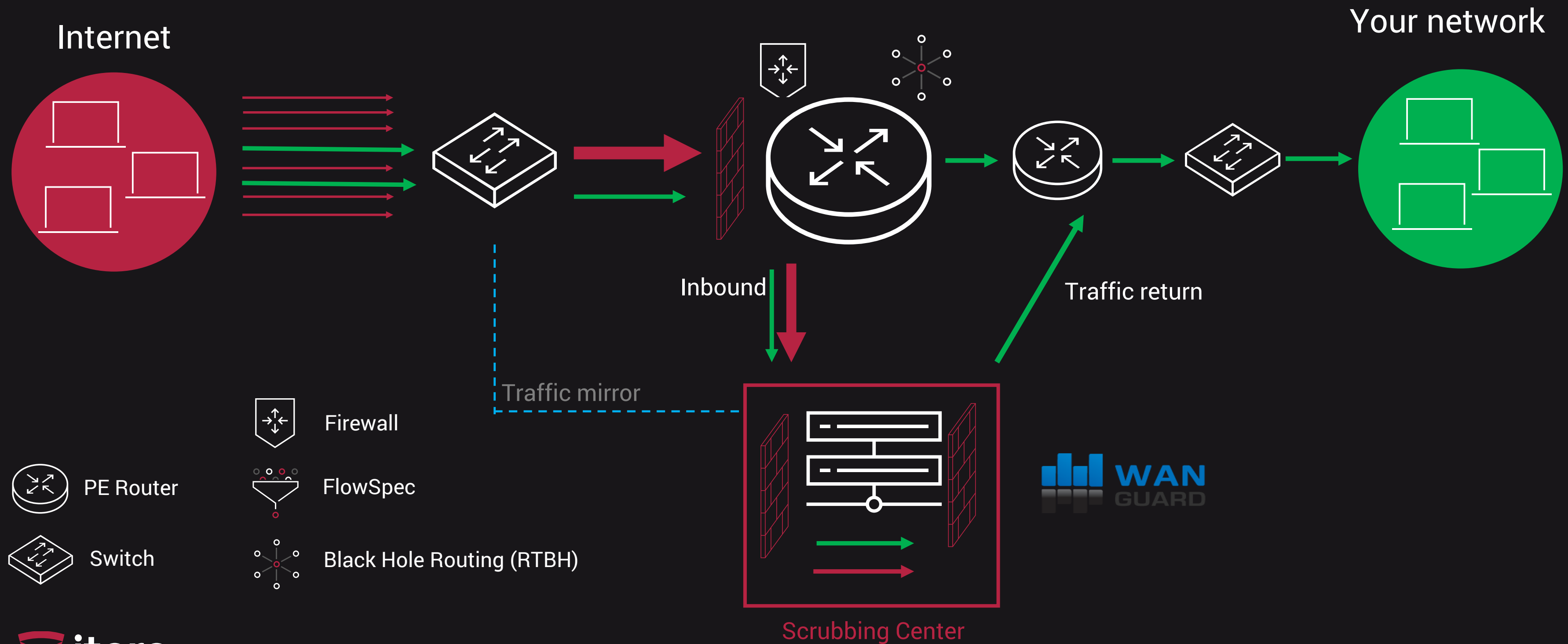
SRX

Check if Your router supports
FlowSpec!

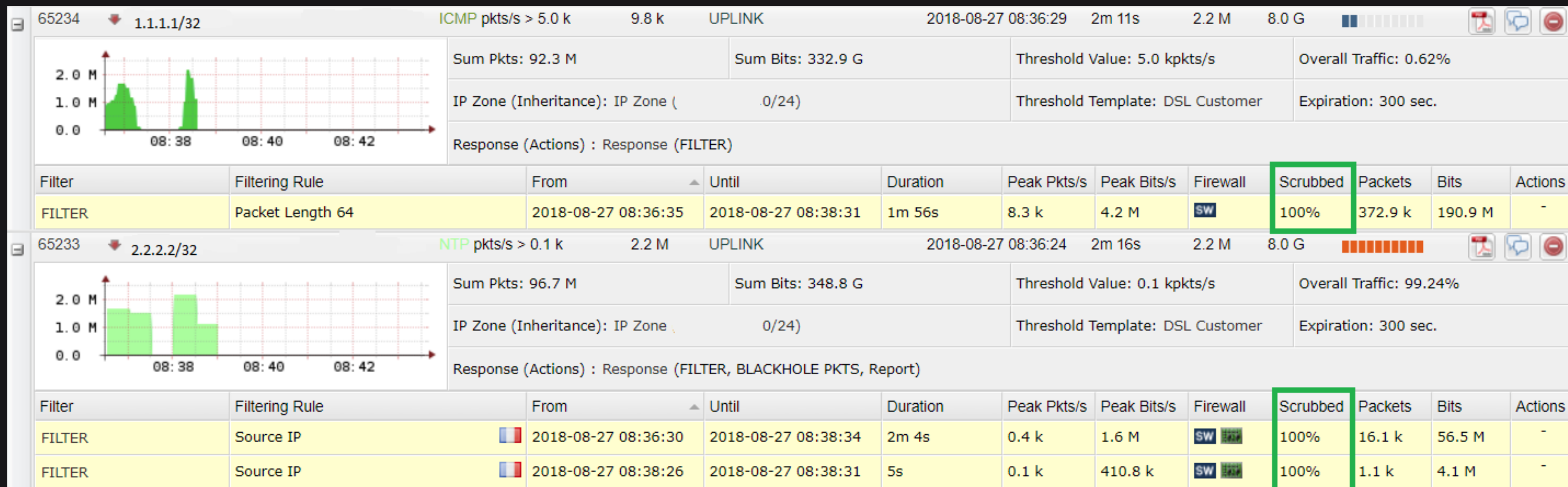
Filtering – 3 stage



Filtering – 2 stage without FlowSpec



Wanguard - Filtering without FlowSpec



Wanguard - Software filtering



Chain wanguard_4_2_0 (0 references)

pkts	bytes	target	prot	opt	in	out	source	destination
------	-------	--------	------	-----	----	-----	--------	-------------

Chain wanguard_custom (1 references)

pkts	bytes	target	prot	opt	in	out	source	destination
------	-------	--------	------	-----	----	-----	--------	-------------

0	0	DROP	udp	--	eth7	*	0.0.0.0/0	0.0.0.0/0
---	---	------	-----	----	------	---	-----------	-----------

multiport sports 123 limit: above 500/sec burst 5

9399K	13G	RETURN	all	--	*	*	0.0.0.0/0	0.0.0.0/0
-------	-----	--------	-----	----	---	---	-----------	-----------

SW Create Software Firewall Rule

Rule Description: NTP Block

Software Firewall

Direction: Inbound

Filter(s): WG FILTER

Packet Matching Rules (Moderate CPU Utilization)

IP Protocol(s): UDP

Src. IP/mask: Any

Src. Port(s): 123

Dst. IP/mask: Any

Dst. Port(s): Any

IP Packet Length: Any

IP TimeToLive: Any

TCP Flags Set:

TCP Flags Unset:

Packet Matching Rules (High CPU Utilization)

Payload Content: Any

Country(ies): Any

Firewall Rule Action

Firewall Policy: Rate Limit

Rate Limit: 500 /second

Rate Limit Hashing:

Firewall Rule Expiration

Rule Active Until: Manually deleted

Anomaly #:

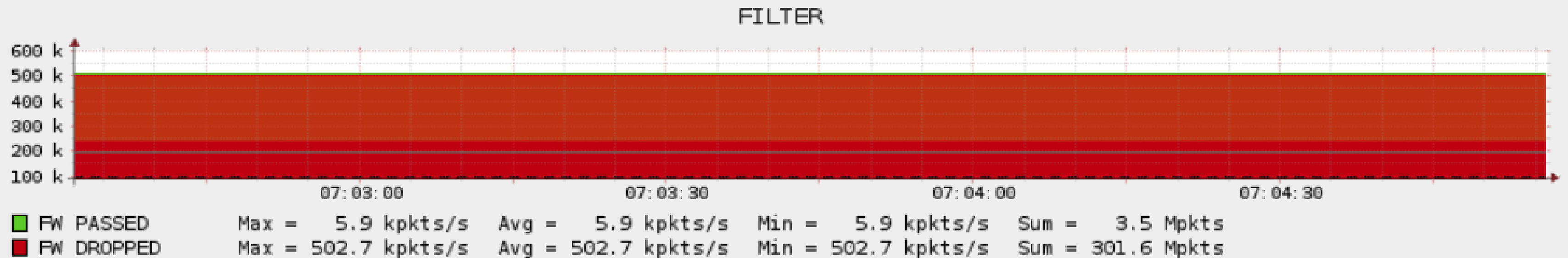
Custom Interval: /minute(s)

Custom Date:

+ Add

Wanguard - Filtering

Mitigation



Filter	Filtering Rule	Started	Latest Alarm	Duration	Scrubbed	Peak Pkts/s (Pkts)	Peak Bits/s (Bits)	Actions
FILTER	Source IP 193	2018-08-26 07:02:37	2018-08-26 07:02:41	4s	100%	247.9 k (6.8 M)	50.2 M (276.5 M)	-
FILTER	Rate Limit Packets	2018-08-26 07:02:27	2018-08-26 07:02:36	9s	100%	161.7 k (1.6 M)	44.3 M (1.2 G)	-
FILTER	Source IP 26	2018-08-26 07:04:08	2018-08-26 07:04:12	4s	100%	130.3 k (5.3 M)	26.5 M (138.9 M)	-
FILTER	Blacklisted IPs	2018-08-26 07:02:27	2018-08-26 07:02:27	-	100%	1 (38)	0.4 k (22.7 k)	-

Wanguard - Hardware filtering



```
#cat /sys/kernel/debug/cxgb4/0000\:05\:00.4/filters
LE-TCAM Filters:
```

```
[[Legend: '!' => locked; '+' => pending set; '-' => pending clear]]
```

Idx	Hits	Hit-Bytes	FCoE	Port	vld:iVLAN	Prot	MPS	Frag
LIP					FIP	LPORT	FPORT	Action
10	823481				0 0/0	0/0	0:0000/0:0000	11/ff 0/0 0/0
00000000/00000000					00000000/00000000	0000/0000	007b/ffff	Drop

Rule Description: NTP DROP

Hardware Firewall

Filter(s): WG FILTER

Packet Matching Rules

IP Protocol(s): UDP

IP Fragment: ☐

Src. IP/mask: Any

Src. Port: 123

Dst. IP/mask: Any

Dst. Port: Any

Firewall Rule Expiration

Rule Active Until: Manually deleted

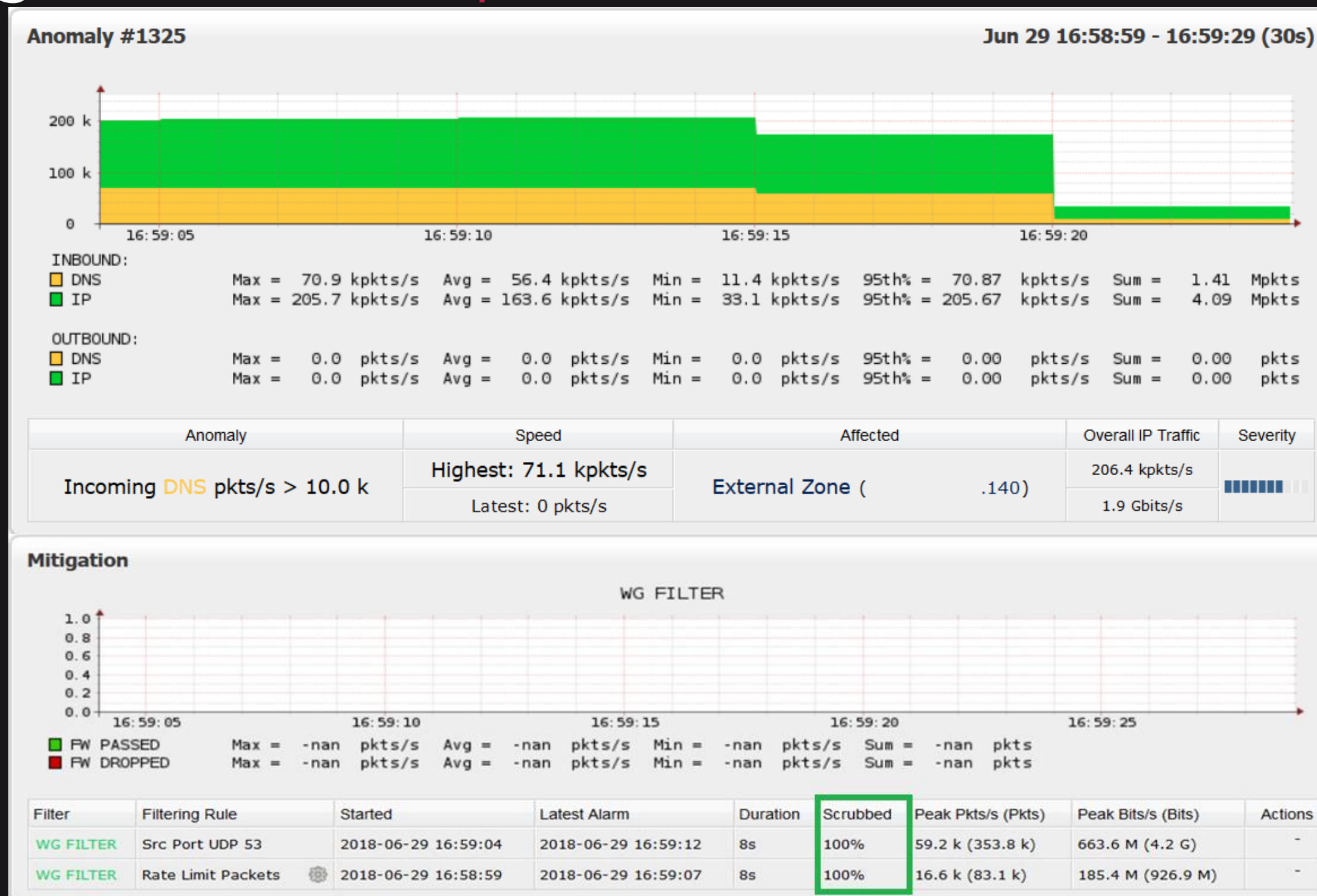
Anomaly #:

Custom Interval: /minute(s)

Custom Date:

+ Add

Wanguard - Filtering with FlowSpec !



Wanguard - Hardware filtering using FlowSpec



```
mx80.lab> show firewall filter __flowspec_default_inet__
```

```
Filter: __flowspec_default_inet__
```

```
Counters:
```

Name	Bytes	Packets
*,1.1.1.1,proto=17,srcport=123	841816	5234116

```
mx80.lab> show route protocol bgp table inetflow.0 extensive
```

```
inetflow.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
```

```
*,1.1.1.1,proto=17,srcport=123/term:2 (1 entry, 1 announced)
```

```
TSI:
```

```
KRT in dfwd;
```

```
Action(s): routing-instance DIRTY-VRF,count
```

```
*BGP Preference: 170/-101
```

```
Next hop type: Fictitious, Next hop index: 0
```

```
Next-hop reference count: 1
```

```
State: <Active Int Ext>
```

```
Local AS: 65000 Peer AS: 65000
```

```
Age: 37
```

```
Task: BGP_65000.10.0.9.66
```

```
Announcement bits (1): 0-Flow
```

```
AS path: I
```

```
Communities: traffic-rate:0:1875
```

```
Accepted
```

```
Localpref: 100
```

```
Router ID: 10.0.9.66
```

Get Wanguard with FlowSpec now !



Instalation

- One router is enough !
- BGP configuration.
- No loop thanks to FlowSpec !
- We prefer VRF over GRE.



Filtering

- Wanguard send FlowSpec rules.
- Automatic filtering with available anti DDoS rules.

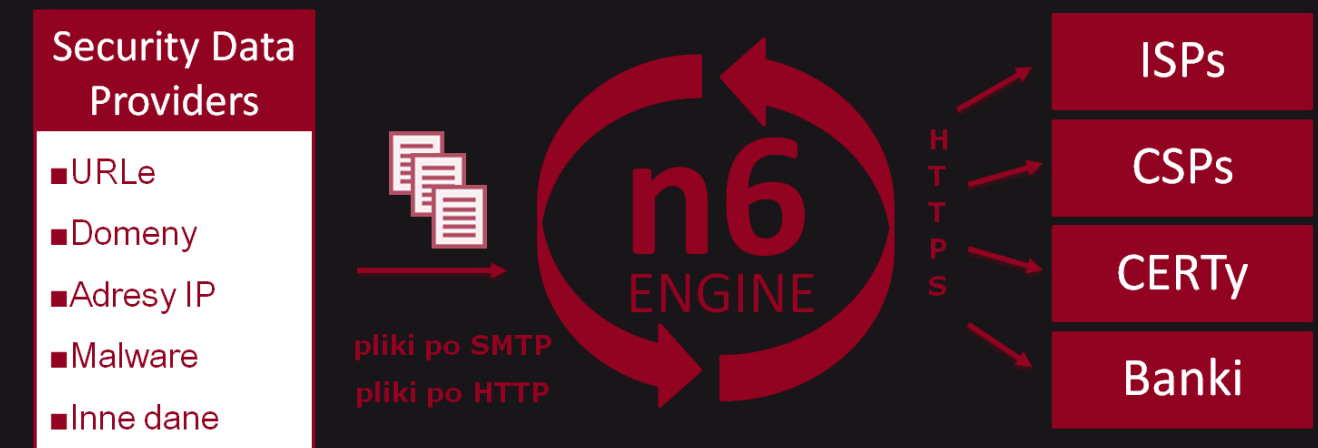


Protection

- Network monitotring.
- After action reports on email.

Ways to effectively reduce DDoS attacks

- Using ShadowServer or regional CERT providers - n6 (Poland)
- Blocking ports used in attacks
- Blocking any spoofing from Your network (Spoofers / RPF) *
- Active scans of Your network (np.: OpenVAS, Suricata)
- Monitoring of outbound traffic



* <https://www.caida.org/projects/spoofers/>



Piotr Okupski

itorio.com.pl