itoro

Multi-stage DDoS filtering with Wanguard, and more

PLONG 21, Kraków 1-2.10.2018 r.

www.itoro.com.pl

PLNOG
where ipeople meet

About ITORO

- **Wanguard implementations (protection agaist DDoS attacks)**
- The only one
- Huge experience

Andrisoft GOLD PARTNER

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

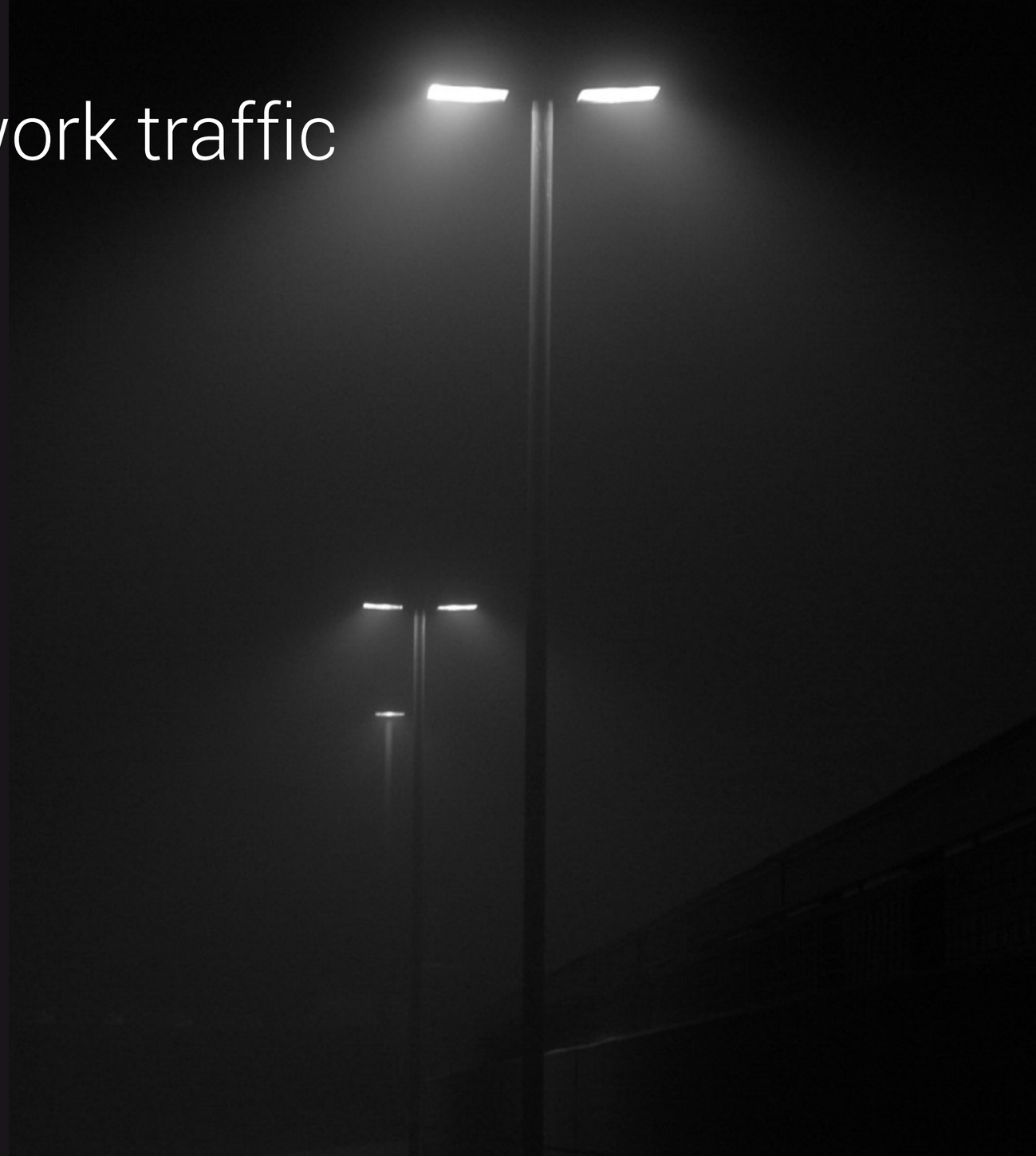
- Full support before and after installation
- Comprehensive service and advice
- Support for IT dept for smooth integration of Wanguard

Methods of collecting network traffic

- Port mirroring
- 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 are we 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

Links

Bandwidth capacity of upstream and peering links.

BGP Policy

BGP Import restrictions, anti-spoofing, BGP BCOP 38.

Dispersion

Dividing the network into smaller segments, source filtering of traffic from EU/World/Regions.

DDoS / WAF protection

Automated reaction to threats.

Monitoring

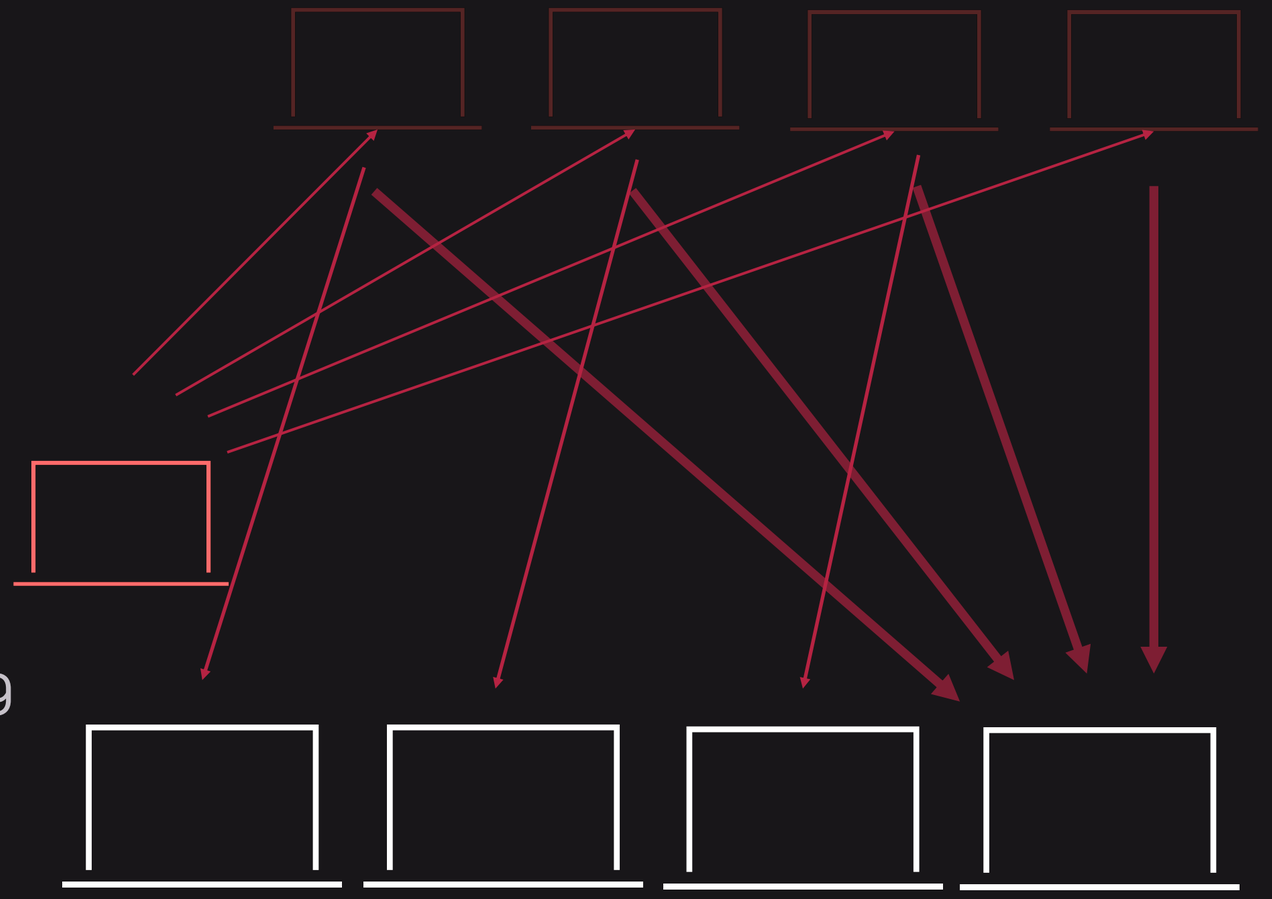
Network traffic monitoring from outside and within the company.

Anti-DDoS action plan

Action plan and procedures.
Public relations – information about an outage/attack.

Services that use DDoS 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



source: https://www.us-cert.gov/ncas/alerts/TA14-017A

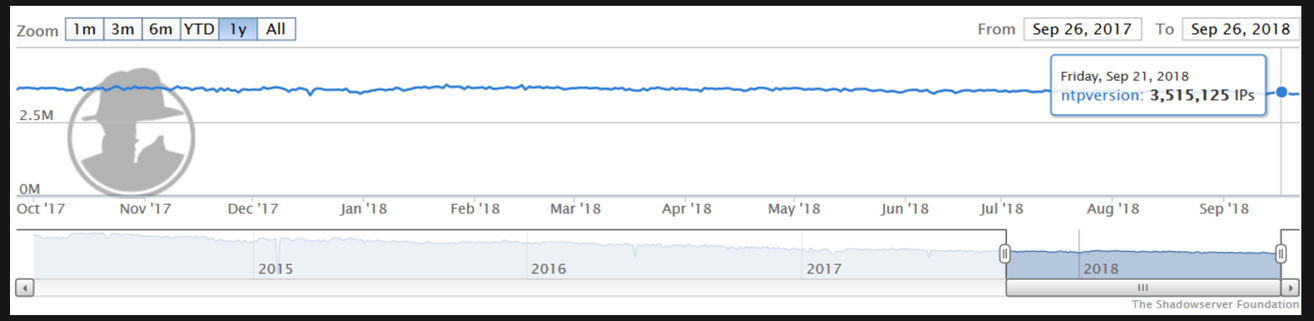
Statistics – should I be scared?

SSDP (UDP/1900)

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

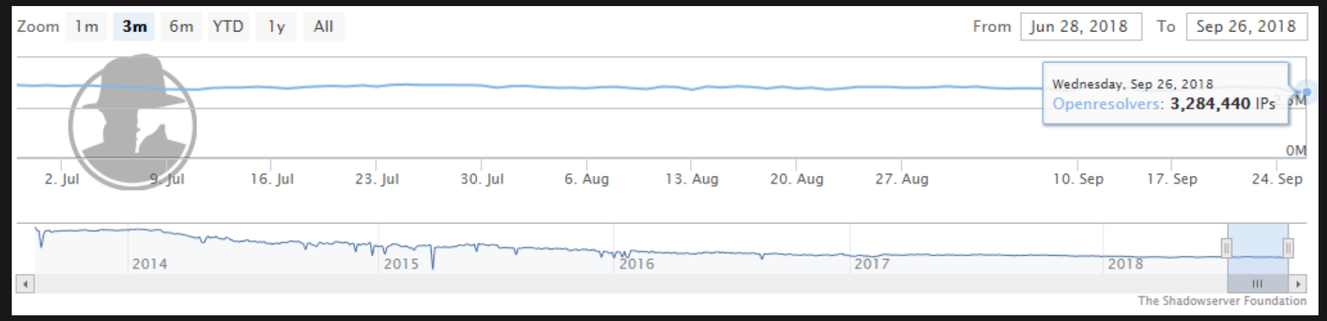
NTP (UDP/123)

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

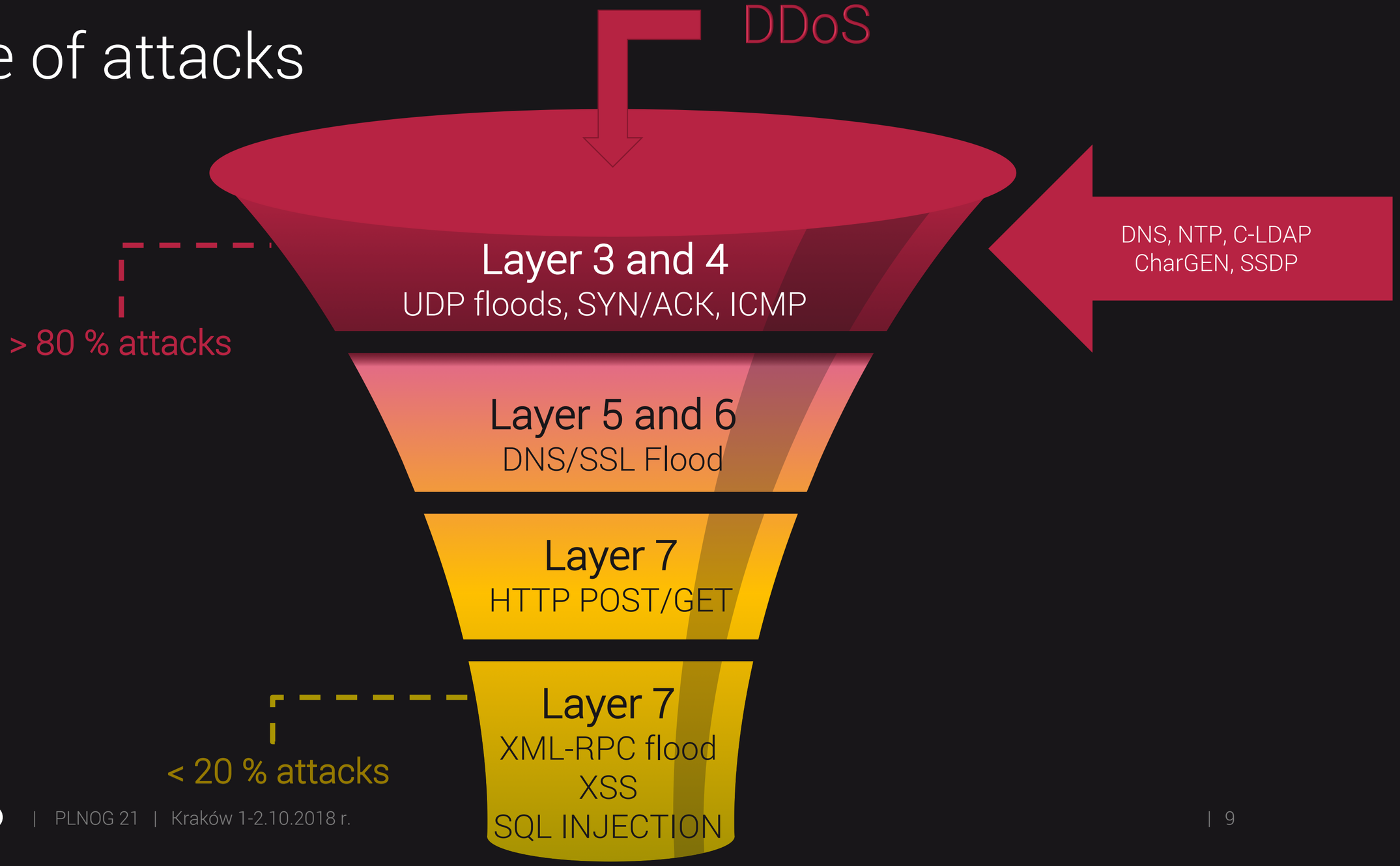


DNS (UDP/53)

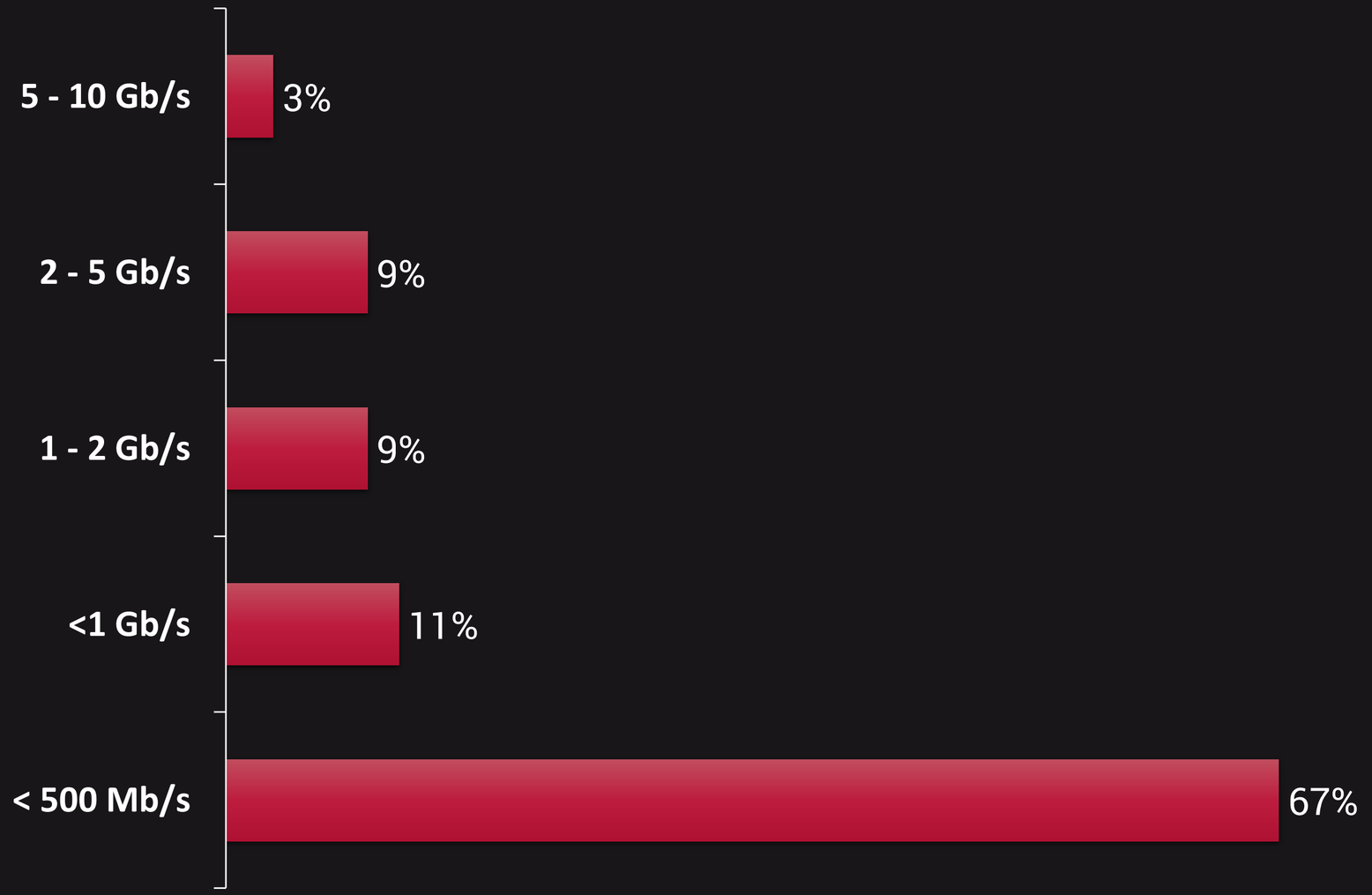
Country	Total
China	1,263,833
United States	319,053
Republic of Korea	164,772
Russian Federation	144,922
Taiwan	115,780



Share of attacks



Attack speeds

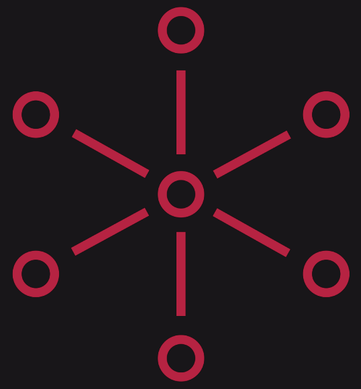


Summary for ISP

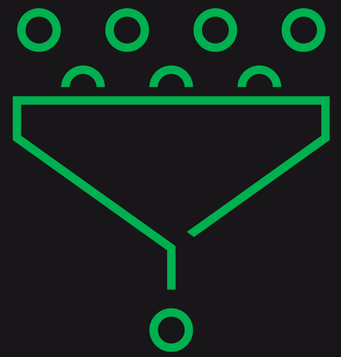
Comments

- ✓ Avg. duration of attacks: <30 seconds on subscribers
- ✓ Avg. duration of attacks on infrastucture: 1-6 hours
- ✓ Multiple attack vectors: NTP/DNS/SSDP/ICMP
- ✓ RTBH less effective, due to carpet bomb attacks

Important terms

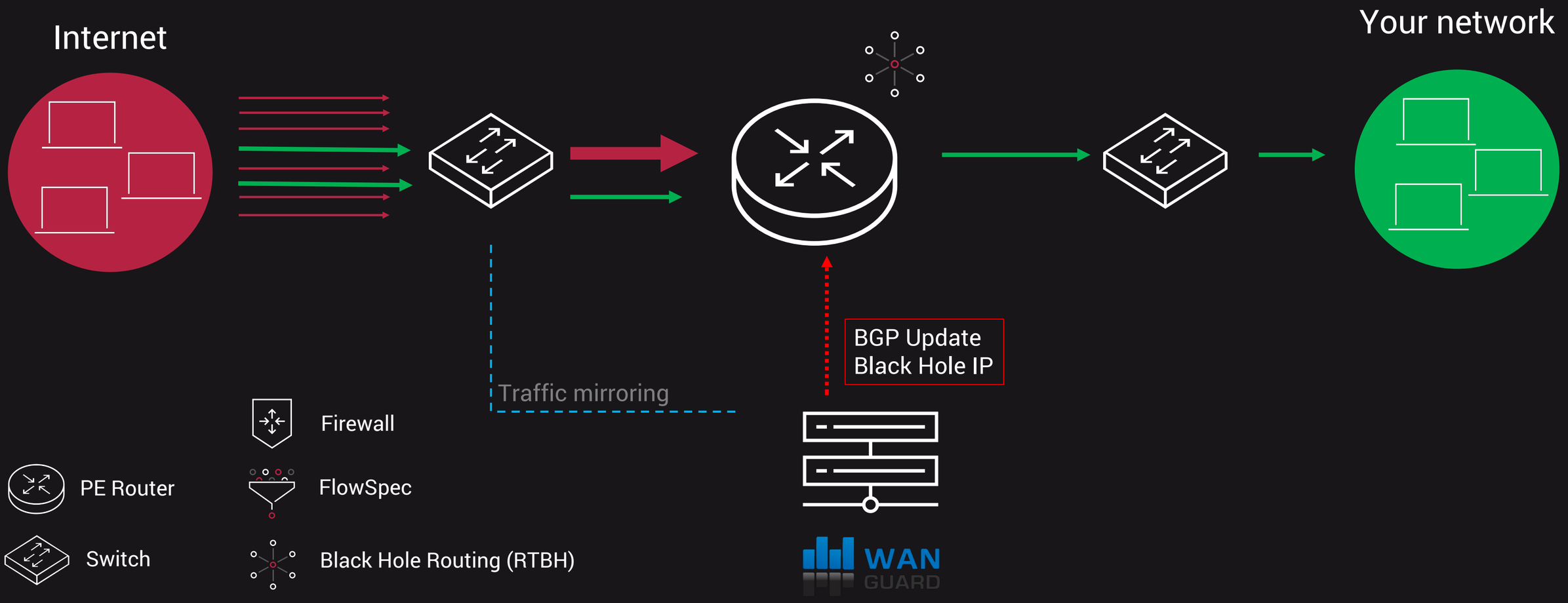


Black Hole Routing (**R**emotely **T**riggered **B**lack **H**ole **R**outing)
The incoming traffic is discarded before entering your network.

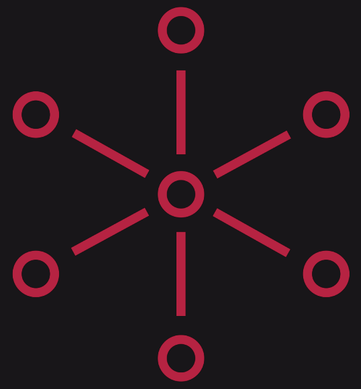


FlowSpec (RFC 5575)
Firewall filter rules are injected into BGP protocol.
Many actions possible:
- drop / limit packets
- redirect
- DSCP (Differentiated Services) used in QoS

Black Hole Routing

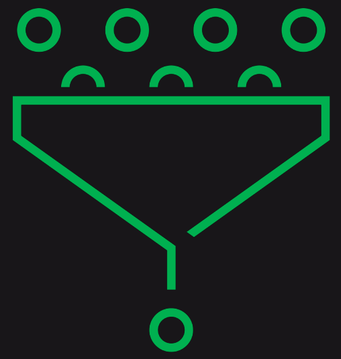


Possibilities of protection against DDoS attacks



Block traffic using **R**emotely **T**riggered **B**lack **H**ole Routing (RTBH)

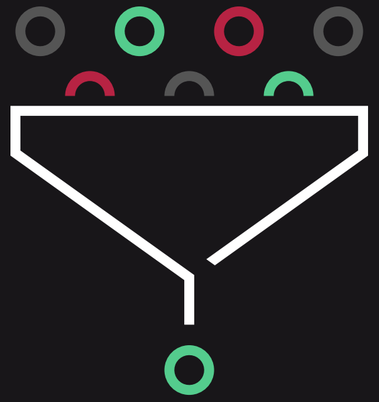
- Black Hole of IP / Network class.
- Selective Black Hole routing (World/Regions/Country/Peering).



Filtering Traffic:

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

FlowSpec



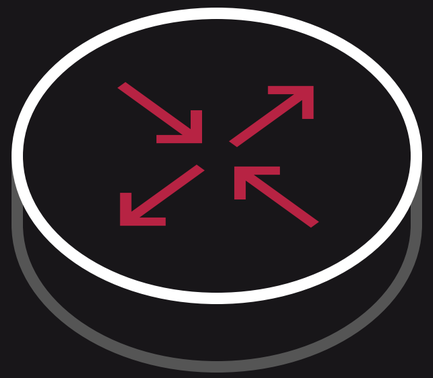
FlowSpec rules :

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

FlowSpec actions:

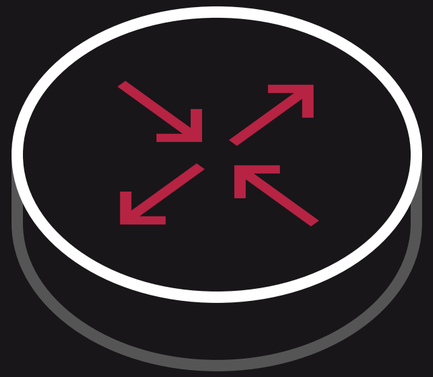
- Traffic limits (example: 10 Mb/s or 0)
- Traffic marking - DSCP
- Redirect - Target VRF (Juniper & Cisco)
- Redirect - IP NextHop (Cisco)

FlowSpec Limitations



CISCO – Maxium 3000 rules

ASR 1xxx
ASR 9xxx
CSR 1000v
CRS-3 (Taiko) LC, CRS-X (Topaz) LC
NCS 5500/6000
XRv 9000

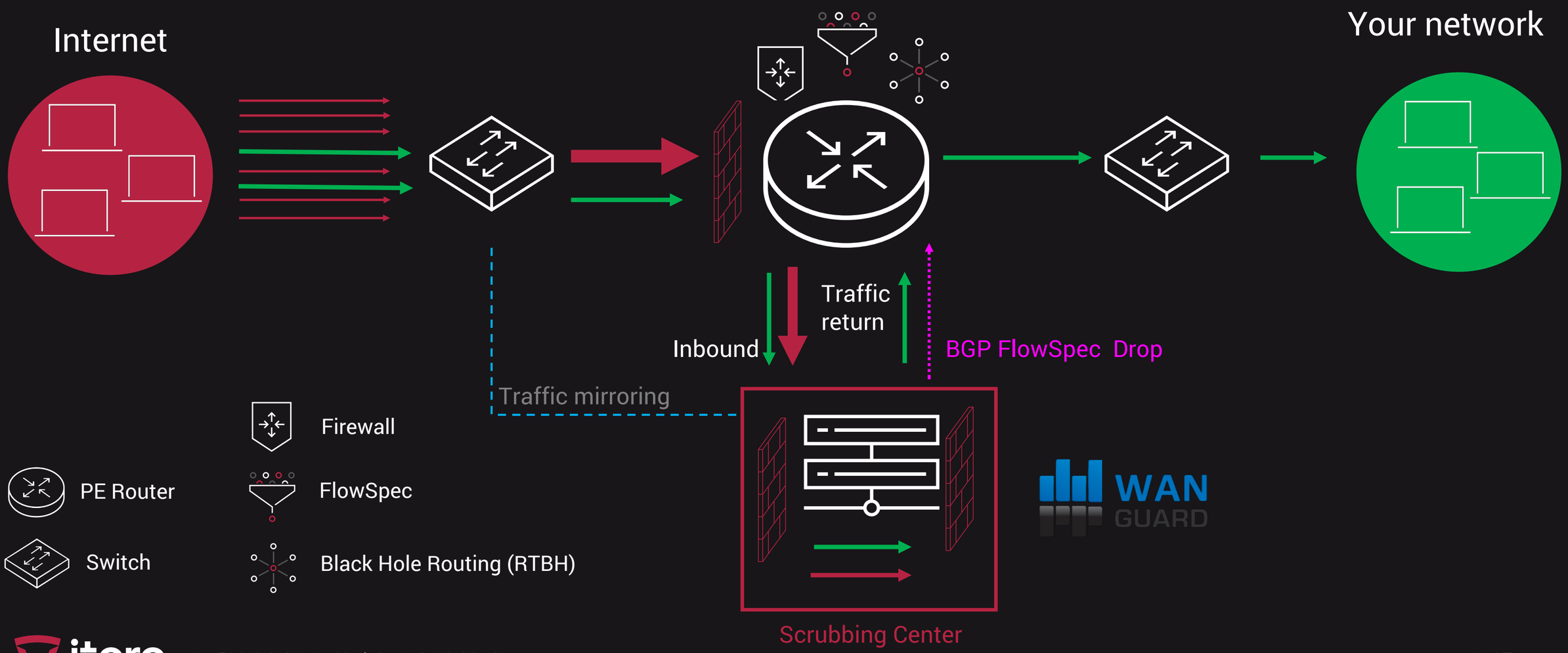


Juniper – Maximum 8000 rules

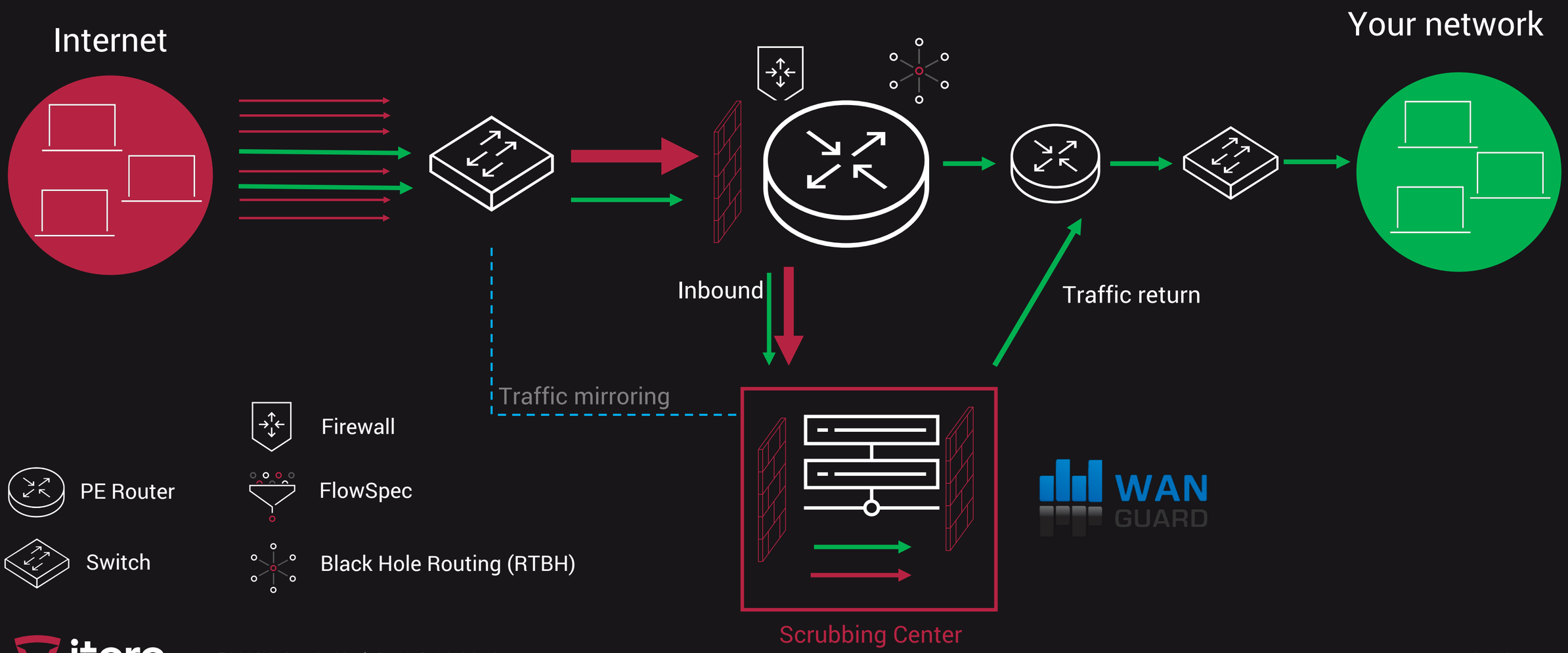
MX series
PTX 10002
QFX 1000[2/8/16]
SRX

Check if your router supports BGP FlowSpec!

Filtering in 3 stages

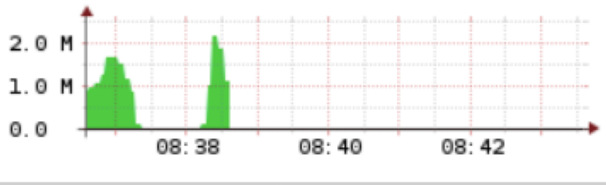


Filtering in 2 stages without FlowSpec



Wanguard - Filtering without FlowSpec

65234 1.1.1.1/32 ICMP pkts/s > 5.0 k 9.8 k UPLINK 2018-08-27 08:36:29 2m 11s 2.2 M 8.0 G



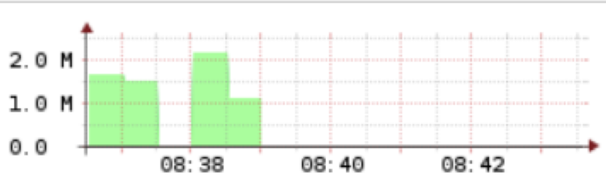
Sum Pkts: 92.3 M | Sum Bits: 332.9 G | Threshold Value: 5.0 kpkts/s | Overall Traffic: 0.62%

IP Zone (Inheritance): IP Zone (0/24) | Threshold Template: DSL Customer | Expiration: 300 sec.

Response (Actions) : Response (FILTER)

Filter	Filtering Rule	From	Until	Duration	Peak Pkts/s	Peak Bits/s	Firewall	Scrubbed	Packets	Bits	Actions
FILTER	Packet Length 64	2018-08-27 08:36:35	2018-08-27 08:38:31	1m 56s	8.3 k	4.2 M	SW	100%	372.9 k	190.9 M	-

65233 2.2.2.2/32 NTP pkts/s > 0.1 k 2.2 M UPLINK 2018-08-27 08:36:24 2m 16s 2.2 M 8.0 G



Sum Pkts: 96.7 M | Sum Bits: 348.8 G | Threshold Value: 0.1 kpkts/s | Overall Traffic: 99.24%

IP Zone (Inheritance): IP Zone 0/24) | Threshold Template: DSL Customer | Expiration: 300 sec.

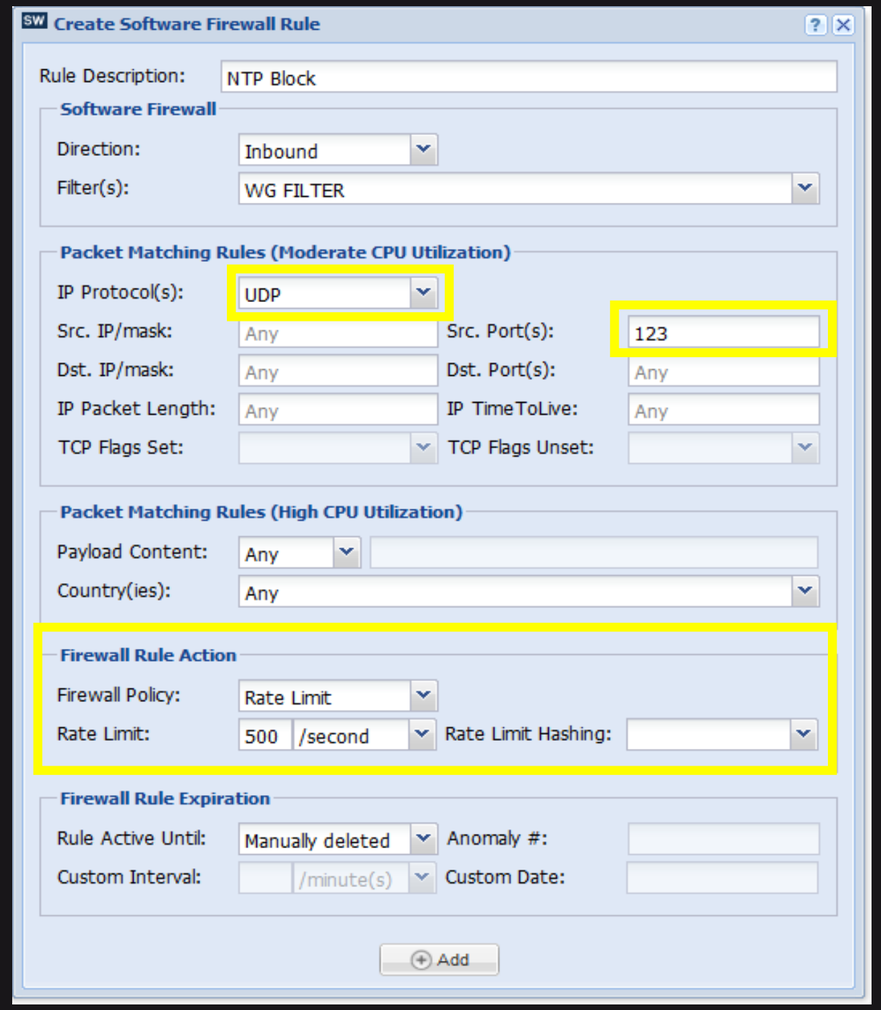
Response (Actions) : Response (FILTER, BLACKHOLE PKTS, Report)

Filter	Filtering Rule	From	Until	Duration	Peak Pkts/s	Peak Bits/s	Firewall	Scrubbed	Packets	Bits	Actions
FILTER	Source IP	2018-08-27 08:36:30	2018-08-27 08:38:34	2m 4s	0.4 k	1.6 M	SW	100%	16.1 k	56.5 M	-
FILTER	Source IP	2018-08-27 08:38:26	2018-08-27 08:38:31	5s	0.1 k	410.8 k	SW	100%	1.1 k	4.1 M	-

Wanguard - Software-based filtering

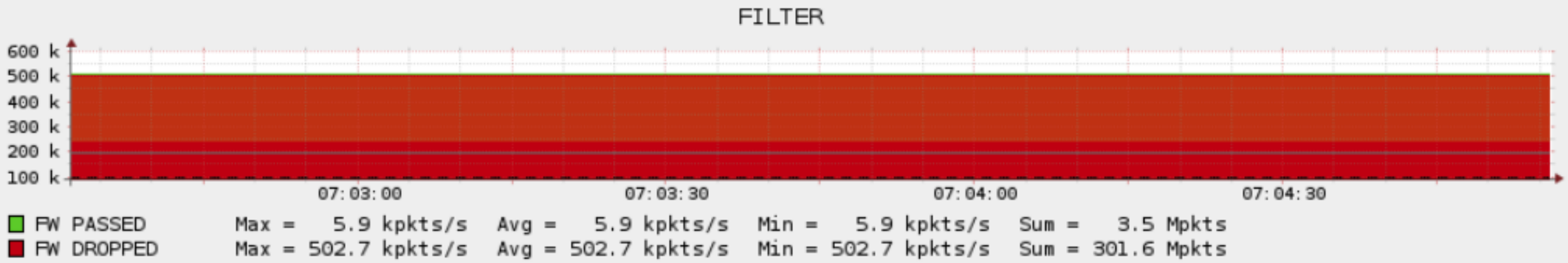
```
Chain wanguard_4_2_0 (0 references)
 pkts bytes target     prot opt in     out     source    destination

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
```



Wanguard - Filtering

Mitigation

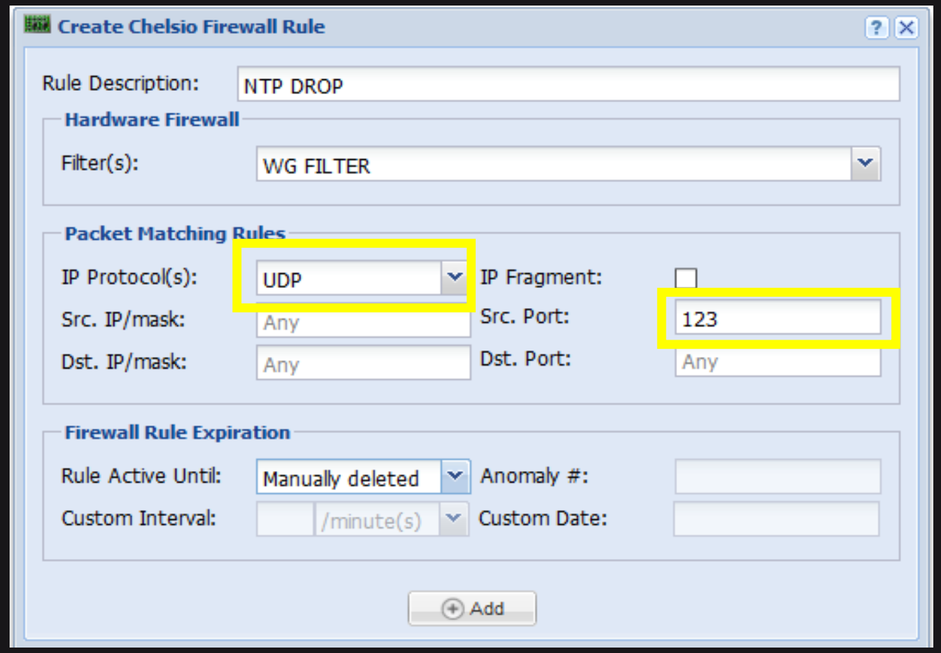


Filter	Filtering Rule		Started	Latest Alarm	Duration	Scrubbed	Peak Pkts/s (Pkts)	Peak Bits/s (Bits)	Actions
FILTER	Source IP	193	2018-08-26 07:02:37	2018-08-26 07:02:41	4s	100%	247.9 k (6.8 M)	50.2 M (276.5 M)	-
FILTER	Rate Limit Packets		2018-08-26 07:02:27	2018-08-26 07:02:36	9s	100%	161.7 k (1.6 M)	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-based filtering

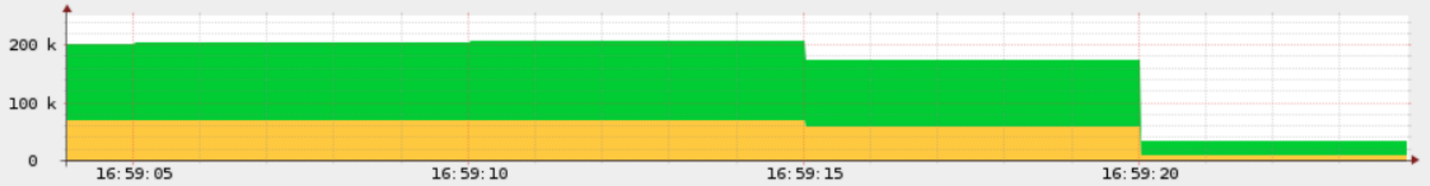
```
#cat /sys/kernel/debug/cxgb4/0000\:05\:00.4/filters
LE-TCAM Filters:

[[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
```



Wanguard - Filtering with FlowSpec !

Anomaly #1325 — **Jun 29 16:58:59 - 16:59:29 (30s)**



INBOUND:

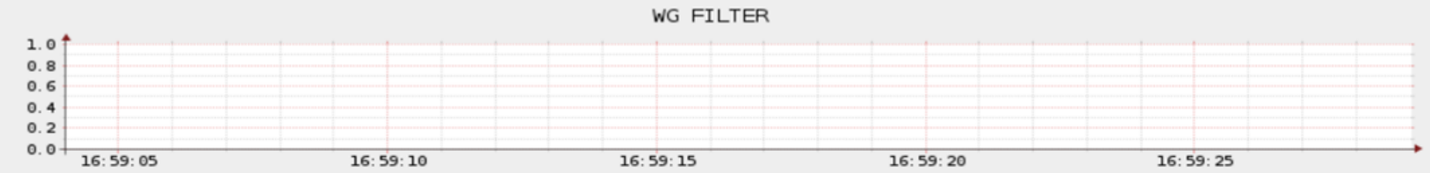
DNS	Max =	70.9	kpkts/s	Avg =	56.4	kpkts/s	Min =	11.4	kpkts/s	95th% =	70.87	kpkts/s	Sum =	1.41	Mpkts
IP	Max =	205.7	kpkts/s	Avg =	163.6	kpkts/s	Min =	33.1	kpkts/s	95th% =	205.67	kpkts/s	Sum =	4.09	Mpkts

OUTBOUND:

DNS	Max =	0.0	pkts/s	Avg =	0.0	pkts/s	Min =	0.0	pkts/s	95th% =	0.00	pkts/s	Sum =	0.00	pkts
IP	Max =	0.0	pkts/s	Avg =	0.0	pkts/s	Min =	0.0	pkts/s	95th% =	0.00	pkts/s	Sum =	0.00	pkts

Anomaly	Speed	Affected	Overall IP Traffic	Severity
Incoming DNS pkts/s > 10.0 k	Highest: 71.1 kpkts/s Latest: 0 pkts/s	External Zone (.140)	206.4 kpkts/s 1.9 Gbits/s	

Mitigation



FW PASSED	Max =	-nan	pkts/s	Avg =	-nan	pkts/s	Min =	-nan	pkts/s	Sum =	-nan	pkts
FW DROPPED	Max =	-nan	pkts/s	Avg =	-nan	pkts/s	Min =	-nan	pkts/s	Sum =	-nan	pkts

Filter	Filtering Rule	Started	Latest Alarm	Duration	Scrubbed	Peak Pkts/s (Pkts)	Peak Bits/s (Bits)	Actions
WG FILTER	Src Port UDP 53	2018-06-29 16:59:04	2018-06-29 16:59:12	8s	100%	59.2 k (353.8 k)	663.6 M (4.2 G)	-
WG FILTER	Rate Limit Packets	2018-06-29 16:58:59	2018-06-29 16:59:07	8s	100%	16.6 k (83.1 k)	185.4 M (926.9 M)	-

Wanguard - FlowSpec-based filtering

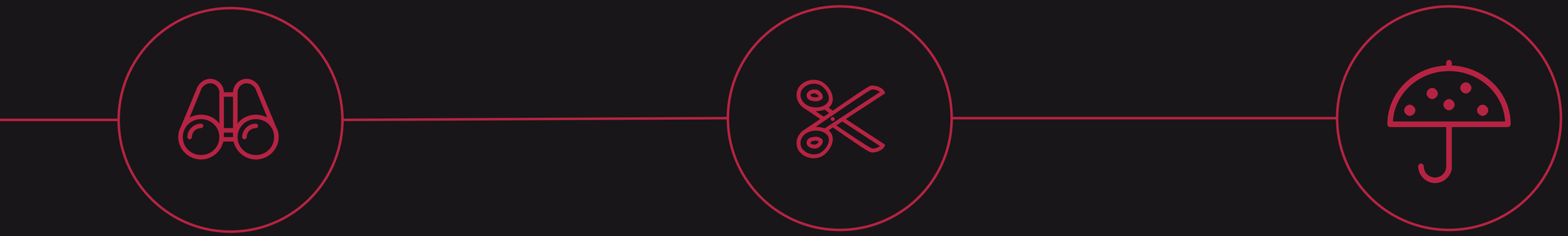
```
mx80.lab> show firewall filter __flowspec_default_inet__

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!



Installation

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

Filtering

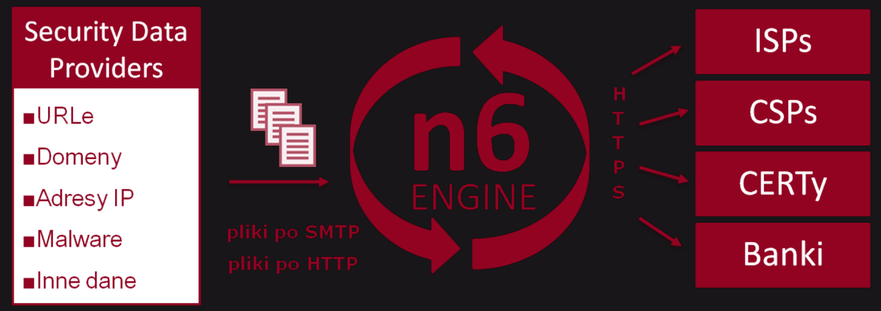
- Wanguard sends FlowSpec rules.
- Automatic filtering with the available anti DDoS rules.

Protection

- Network monitoring.
- Detailed reports via 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 (Spoofer / RPF) *
- Active scans of your network (np.: OpenVAS, Suricata)
- Monitoring of outbound traffic



* https://www.caida.org/projects/spoofer/

Piotr Okupski

itoro.com.pl