MYNOG-1

Managing DDOS :

JARING’s DDOS experience

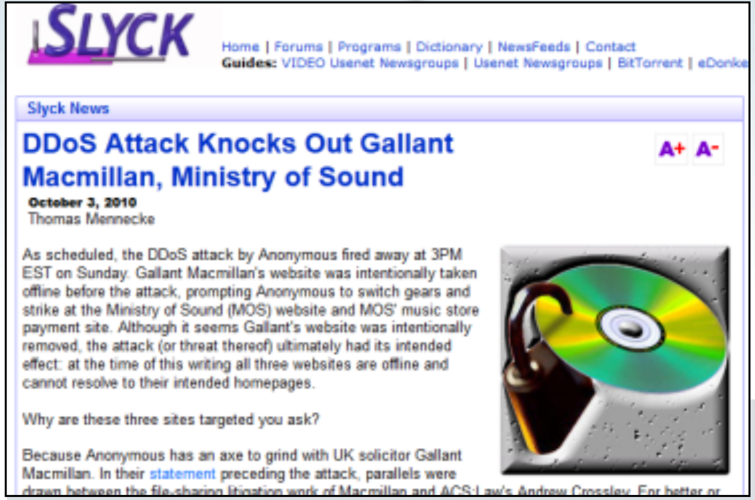
Prepared by : Zamzuri Zainuddin (Corporate Access)
Date : Jan 16, 2012

Agenda :

1) Refresher : Intro to DDOS
2) JARING’s experience in early 2000
3) The use of RTBH : Simple vs Advanced
4) The end to end services (FW/QoS)
5) The deployment of DDOS Armour
6) The outcome ?

JARING come together

News on DDOS



SLYCK
Home | Forums | Programs | Dictionary | NewsFeeds | Contact
Guides: VIDEO Usenet Newsgroups | Usenet Newsgroups | BitTorrent | eDonke
Slyck News
A+ A-

DDoS Attack Knocks Out Gallant Macmillan, Ministry of Sound

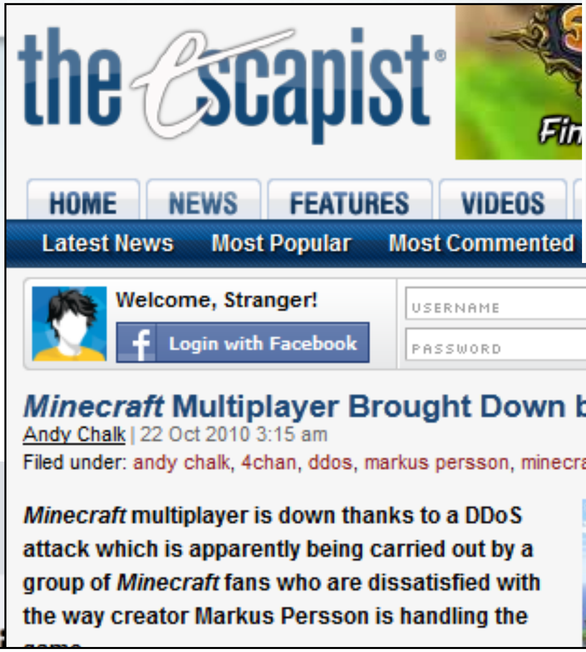
October 3, 2010
Thomas Mennecke

As scheduled, the DDoS attack by Anonymous fired away at 3PM EST on Sunday. Gallant Macmillan's website was intentionally taken offline before the attack, prompting Anonymous to switch gears and strike at the Ministry of Sound (MOS) website and MOS' music store payment site. Although it seems Gallant's website was intentionally removed, the attack (or threat thereof) ultimately had its intended effect: at the time of this writing all three websites are offline and cannot resolve to their intended homepages.

Why are these three sites targeted you ask?

Because Anonymous has an axe to grind with UK solicitor Gallant Macmillan. In their statement preceding the attack, parallels were drawn between the file-sharing litigation work of Macmillan and ACS:Law's Andrew Crossley. For better or

Bloomberg News: Amazon's EC2 used DDoS Attack on SONY's PSN

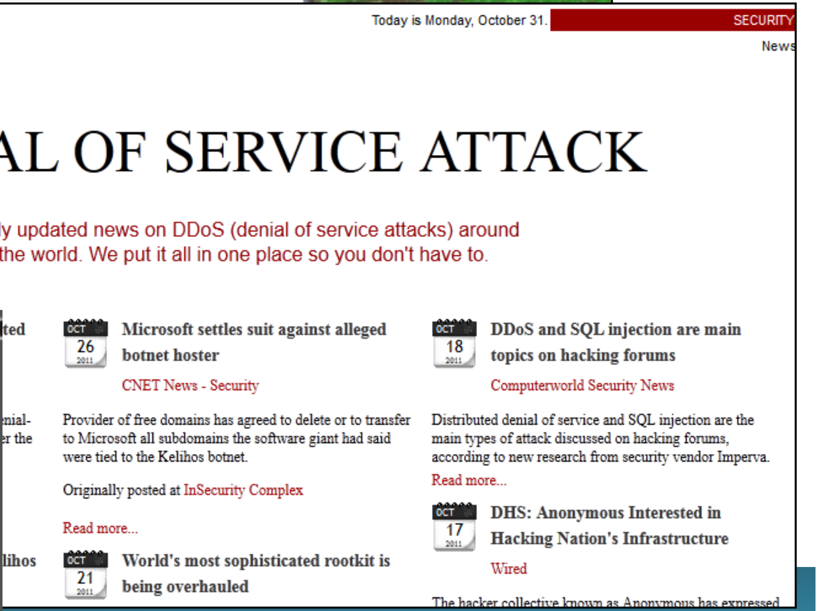


Minecraft Multiplayer Brought Down by DDoS Attack

Andy Chalk | 22 Oct 2010 3:15 am
Filed under: andy chalk, 4chan, ddos, markus persson, minecraft, notch

Minecraft multiplayer is down thanks to a DDoS attack which is apparently being carried out by a group of *Minecraft* fans who are dissatisfied with the way creator Markus Persson is handling the game.

IRC.ANONOPS.LI
#OPMALAYSIA
PORT: 6667
WEDNESDAY,
JUNE 15
7 : 30 PM
GMT
Operation Malaysia
TARGET: HTTP://WWW.MALAYSIA.GOV.MY
OPERATION MALAYSIA



Protect your site now! Visit DOSarrest
Today is Monday, October 31.
SECURITY
Resources
News

DENIAL OF SERVICE ATTACK

Daily updated news on DDoS (denial of service attacks) around the world. We put it all in one place so you don't have to.

ted

nial-
r the

lihos

OCT 26 2011 **Microsoft settles suit against alleged botnet hoster**

CNET News - Security

Provider of free domains has agreed to delete or to transfer to Microsoft all subdomains the software giant had said were tied to the Kelihos botnet.

Originally posted at InSecurity Complex

Read more...

OCT 21 2011 **World's most sophisticated rootkit is being overhauled**

OCT 18 2011 **DDoS and SQL injection are main topics on hacking forums**

Computerworld Security News

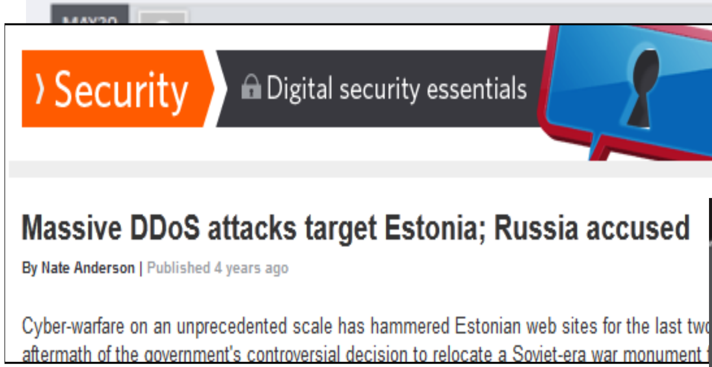
Distributed denial of service and SQL injection are the main types of attack discussed on hacking forums, according to new research from security vendor Imperva.

Read more...

OCT 17 2011 **DHS: Anonymous Interested in Hacking Nation's Infrastructure**

Wired

The hacker collective known as Anonymous has expressed



Massive DDoS attacks target Estonia; Russia accused

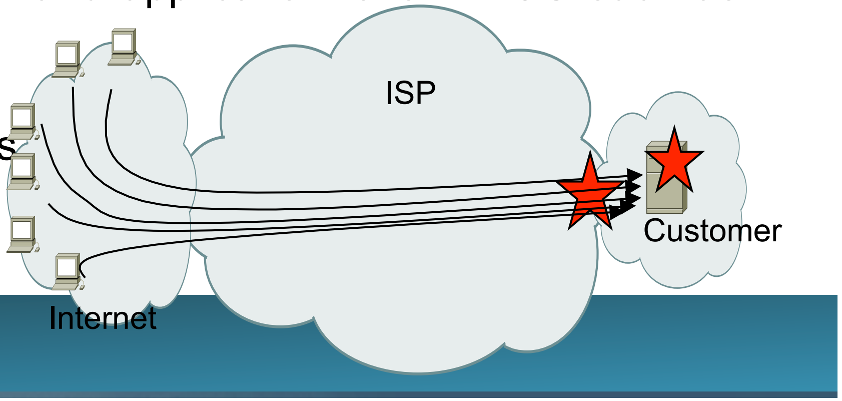
By Nate Anderson | Published 4 years ago

Cyber-warfare on an unprecedented scale has hammered Estonian web sites for the last two aftermath of the government's controversial decision to relocate a Soviet-era war monument

What is DDOS ?

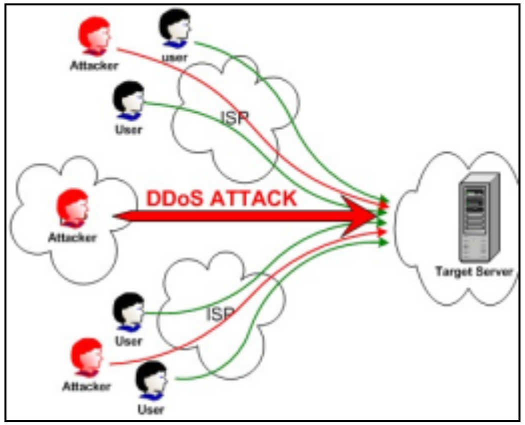
A **Distributed Denial of Service Attack (DDoS)** occurs when massive attackers' traffic **floods targeted resource** or system, making it unavailable or unstable due to not having enough resources to serve legitimate sessions. These origin systems are compromised by :

- ○ **Malware/Trojan**, that can trigger compromised systems to send illegitimate traffic based on time/date/duration.
- ○ **Reflected attacks (by Botnet)**, that send forged requests to computers and reply to those requests with unnecessary big packet payload and high duplication rate at parallel times (amplification).
- ○ ICMP+Ping+SYN Flood by **misconfigured network devices** which allow root commands.
- ○ **Teardrop attacks** of misaligned IP Fragment and application level DDOS such as IRC taking advantage of buffer overflow.
- ○ Any **applications that trigger DDOS**, such as rDOS, Port-Scanner, IP-Hiding tool, LOIC, SQL Slammer,etc.



What will happen to customers ?

- DDOS attacks normally target a single IP (or few IPs) in prolonged or intermittent patterns causing **collateral damage** to the customer business.
- The server under attack (web hosting service, etc) will become unavailable and **registers downtime**. Any service attached to the server will be highly affected.
- This **impacts their business** continuity as they enjoy lower availability index. This can also impact directly to the lower revenue in the long run.



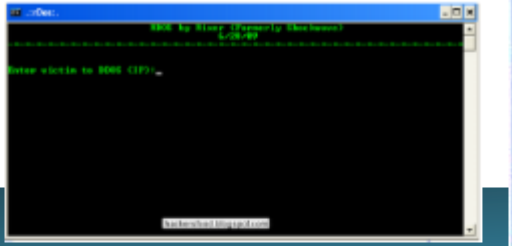
How to protect ?

To the ISP :

- Service providers normally use **Blackhole/Sinkholing** as a mean to protect the network.
- This is done by **redirecting** all traffic attached to an identified IP address to a sinking device (normally a router/server).
- More advance technique of **scrubbing** can also be used.

To the customer :

- The customers normally have **firewalls/IDS/IPS** to protect basic DDOS attacks.
- Customers also can deploy **powerful high end server** (CPU/Memory) that can "sustain" the attacks at some levels.
- They can also have "**large**" **WAN capacity** to sustain DDOS attacks (however, too expensive).



```
Enter victim to DDOS (IP):_
```

The challenges for Service Providers ?

- To **find the destination IP address** under attack. Sometimes, this is difficult to troubleshoot since "**in band**" traffic method is used, which might be the same paths of the DDOS.
- **Quickly drop the traffic** without any advance and complicated configurations.
- To find a simpler method that requires **easy operation and support.**

Agenda :

1) Refresher : Intro to DDOS
2) JARING's experience in early 2000
3) The use of RTBH : Simple vs Advanced
4) The end to end services (FW/QoS)
5) The deployment of DDOS Armour
6) The outcome ?

JARING's Early Experience

Occurrences of DDOS events are not new. Those were handled by Network Operation Team NOC (pre/post year 2000) :

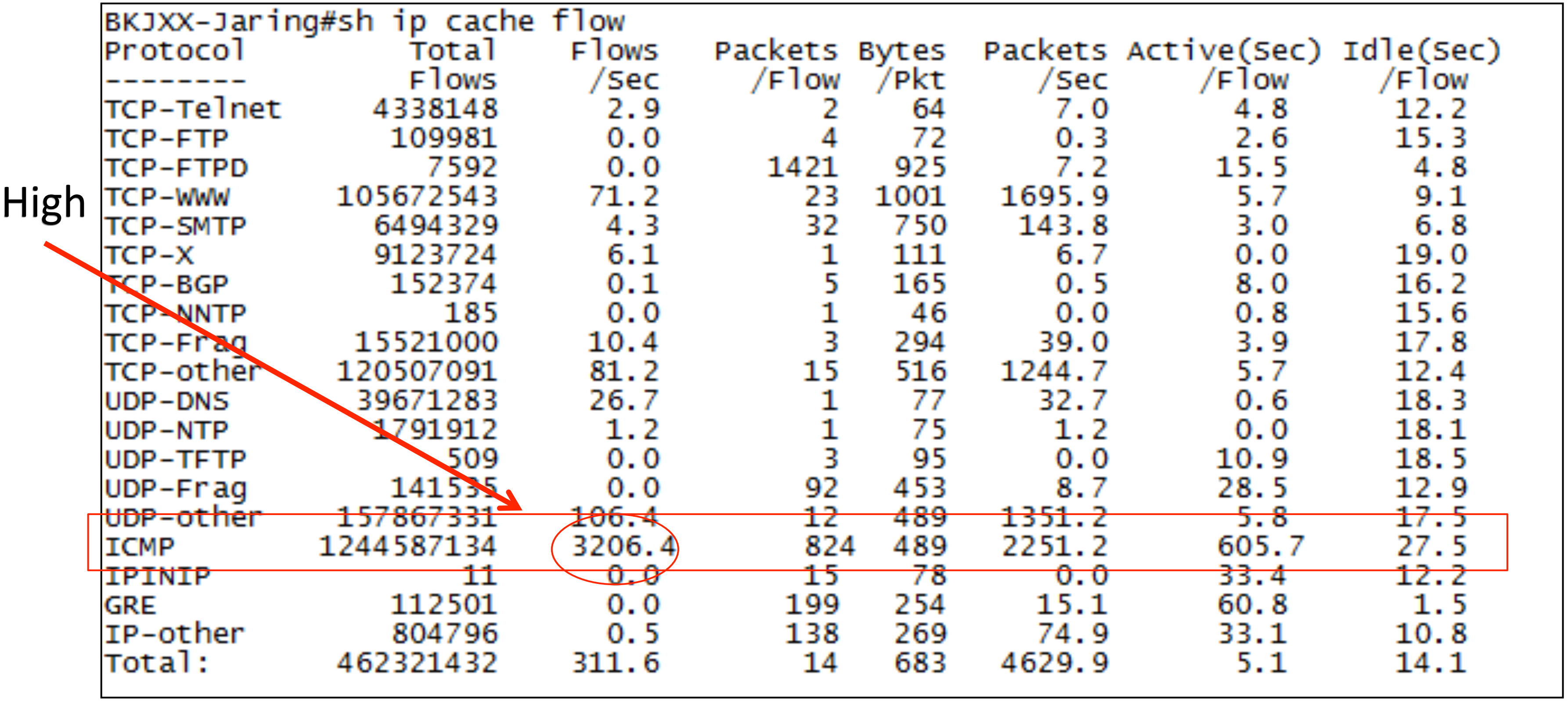
The patterns :

- The DDOS destination is normally **customer's IP** address.
- Sometimes, we did receive attacks destined for **Infrastructure resource**. However the number is small.
- Some of the DDOS attacks are small in volume (Kbps or several mbps).

JARING's Early Experience

The patterns (continues):

- Some of the attacks can be also quite large, and impact network resource. Normally, basic **Netflow** information is needed.



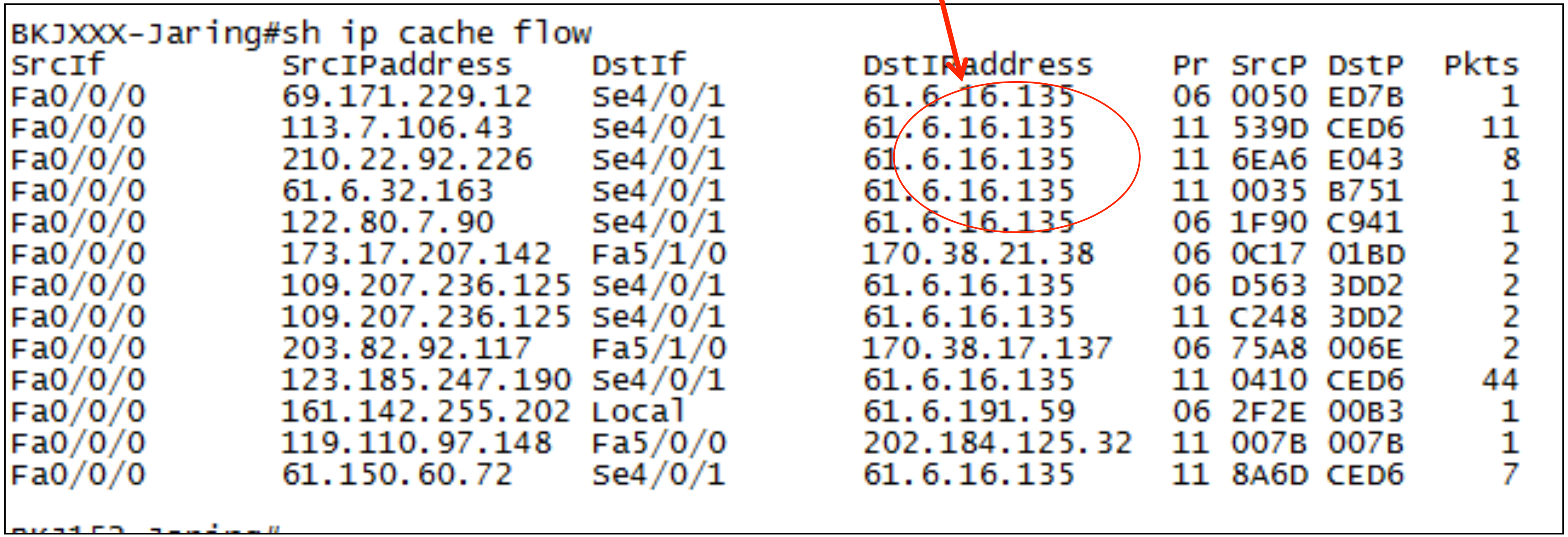
High

```
BKJXX-Jaring#sh ip cache flow
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet     4338148       2.9         2    64      7.0       4.8      12.2
TCP-FTP         109981       0.0         4    72      0.3       2.6      15.3
TCP-FTPD          7592       0.0      1421   925      7.2      15.5       4.8
TCP-WWW      105672543      71.2        23  1001   1695.9       5.7       9.1
TCP-SMTP       6494329       4.3        32   750    143.8       3.0       6.8
TCP-X          9123724       6.1         1   111      6.7       0.0      19.0
TCP-BGP         152374       0.1         5   165      0.5       8.0      16.2
TCP-NNTP           185       0.0         1    46      0.0       0.8      15.6
TCP-Frag      15521000      10.4         3   294     39.0       3.9      17.8
TCP-other    120507091      81.2        15   516   1244.7       5.7      12.4
UDP-DNS       39671283      26.7         1    77     32.7       0.6      18.3
UDP-NTP        1791912       1.2         1    75      1.2       0.0      18.1
UDP-TFTP           509       0.0         3    95      0.0      10.9      18.5
UDP-Frag        141535       0.0        92   453      8.7      28.5      12.9
UDP-other    157867331     106.4        12   489   1351.2       5.8      17.5
ICMP        1244587134    3206.4       824   489   2251.2     605.7      27.5
IPINIP              11       0.0        15    78      0.0      33.4      12.2
GRE             112501       0.0       199   254     15.1      60.8       1.5
IP-other        804796       0.5       138   269     74.9      33.1      10.8
Total:       462321432     311.6        14   683   4629.9       5.1      14.1
```

JARING's Early Experience

- For detail analysis, we use simple **Netflow** output to identify the specific IP that originates the attacks. Applying **ACL** will do the trick at border routers :

Common IP



```
BKJXXX-Jaring#sh ip cache flow
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0/0        69.171.229.12   Se4/0/1        61.6.16.135     06 0050 ED7B     1
Fa0/0/0        113.7.106.43    Se4/0/1        61.6.16.135     11 539D CED6    11
Fa0/0/0        210.22.92.226   Se4/0/1        61.6.16.135     11 6EA6 E043     8
Fa0/0/0        61.6.32.163     Se4/0/1        61.6.16.135     11 0035 B751     1
Fa0/0/0        122.80.7.90     Se4/0/1        61.6.16.135     06 1F90 C941     1
Fa0/0/0        173.17.207.142  Fa5/1/0        170.38.21.38    06 0C17 01BD     2
Fa0/0/0        109.207.236.125 Se4/0/1        61.6.16.135     06 D563 3DD2     2
Fa0/0/0        109.207.236.125 Se4/0/1        61.6.16.135     11 C248 3DD2     2
Fa0/0/0        203.82.92.117   Fa5/1/0        170.38.17.137   06 75A8 006E     2
Fa0/0/0        123.185.247.190 Se4/0/1        61.6.16.135     11 0410 CED6    44
Fa0/0/0        161.142.255.202 Local          61.6.191.59     06 2F2E 00B3     1
Fa0/0/0        119.110.97.148  Fa5/0/0        202.184.125.32  11 007B 007B     1
Fa0/0/0        61.150.60.72    Se4/0/1        61.6.16.135     11 8A6D CED6     7

BK3153-Jaring#
```

JARING’s Early Experience

- For **ACL mitigation**, it is normally deploy at regional and border routers. For example, during mitigating Nachi/Blaster attacks in Oct 2003, we deployed below simple config :

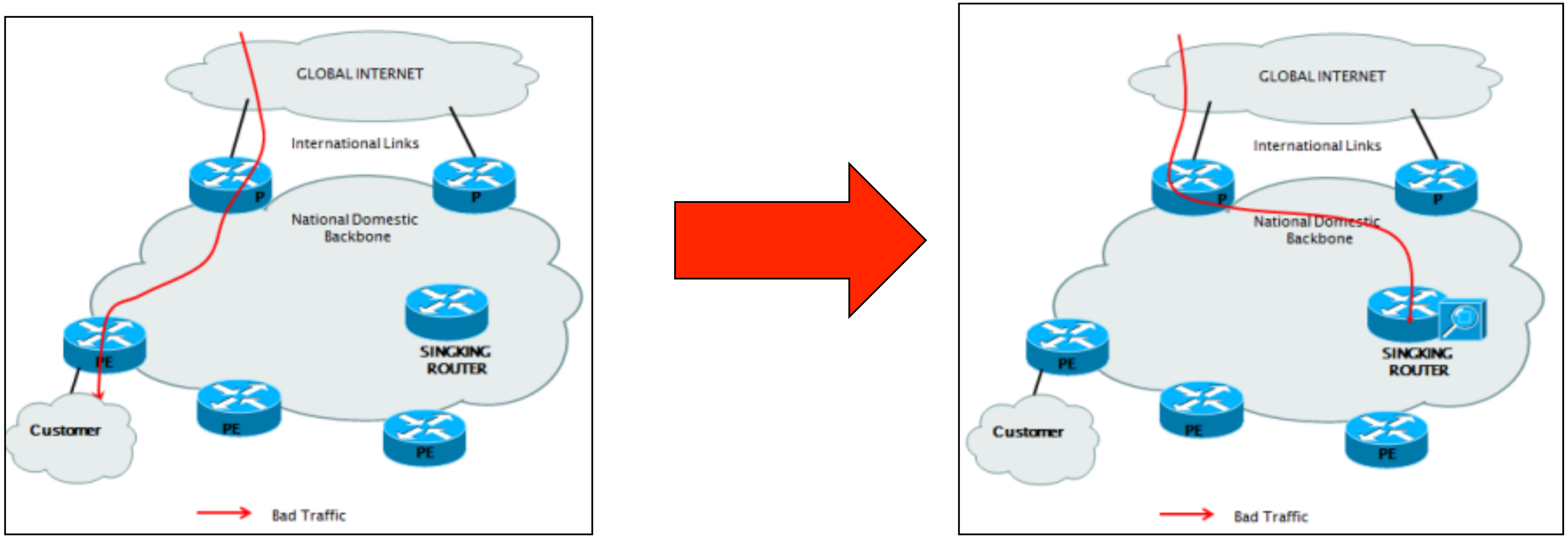
```
access-list 199 permit icmp any any echo
access-list 199 permit icmp any any echo-reply

route-map nachi-worm permit 10
  !--- Match ICMP echo requests and replies (types 0 and 8).
  match ip address 199
  !--- Match 92-byte packets.
  match length 92 92
  !--- Drop the packet.
  set interface Null0

interface XXX
  !--- Apply PBR to the interface.
  ip policy route-map nachi-worm
```

JARING's Early Experience

We used a simple Sinking router to block the attack :

- Sample config of using basic OSPF/Static route in a sinking router (or ISIS/EIGRP) :

```
redistribute static
!
ip route 61.6.16.135 255.255.255.255 Null0
```



Why not enough protection ?

- Previous technique is easy to setup by having one sinkhole router. However, it **consumes precious resource** of transit domestic routes within JARING.

- Preferably, it is more advantageous if we could **drop bad traffic at the earlier**, meaning, at the nearest to border routers.

- Hence, transit **domestic backbones** are protected.

The use of RTBH

- In year 2004, there was an **ISP security** Bootcamp/ seminar organized by Cisco that opened up our eyes on the importance of managing the DDOS events in a coordinated way.

- The security seminar was conducted by **Barry Green** (Cisco) as the instructor, a well known figure of security architect and specialist.

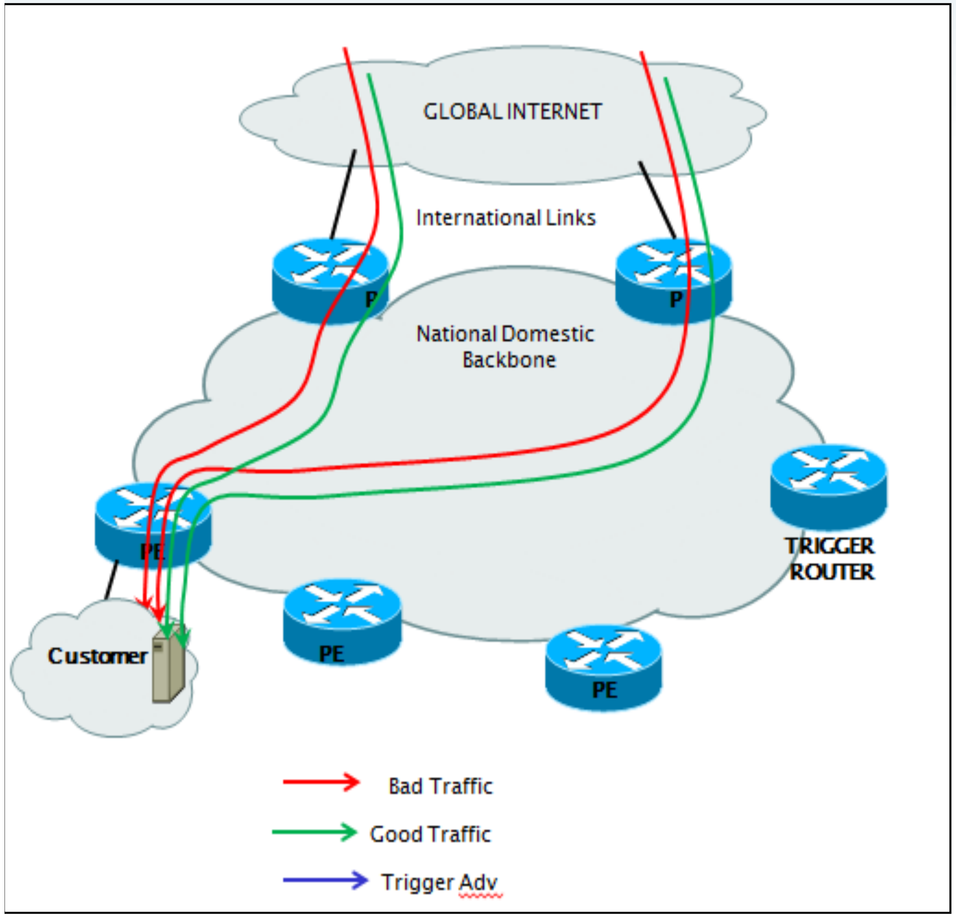
- Apart from having ACL and Netflow info at border routers as a mean to combat DDOS, we were exposed to the use of other effective techniques to deploy (**RTBH**).

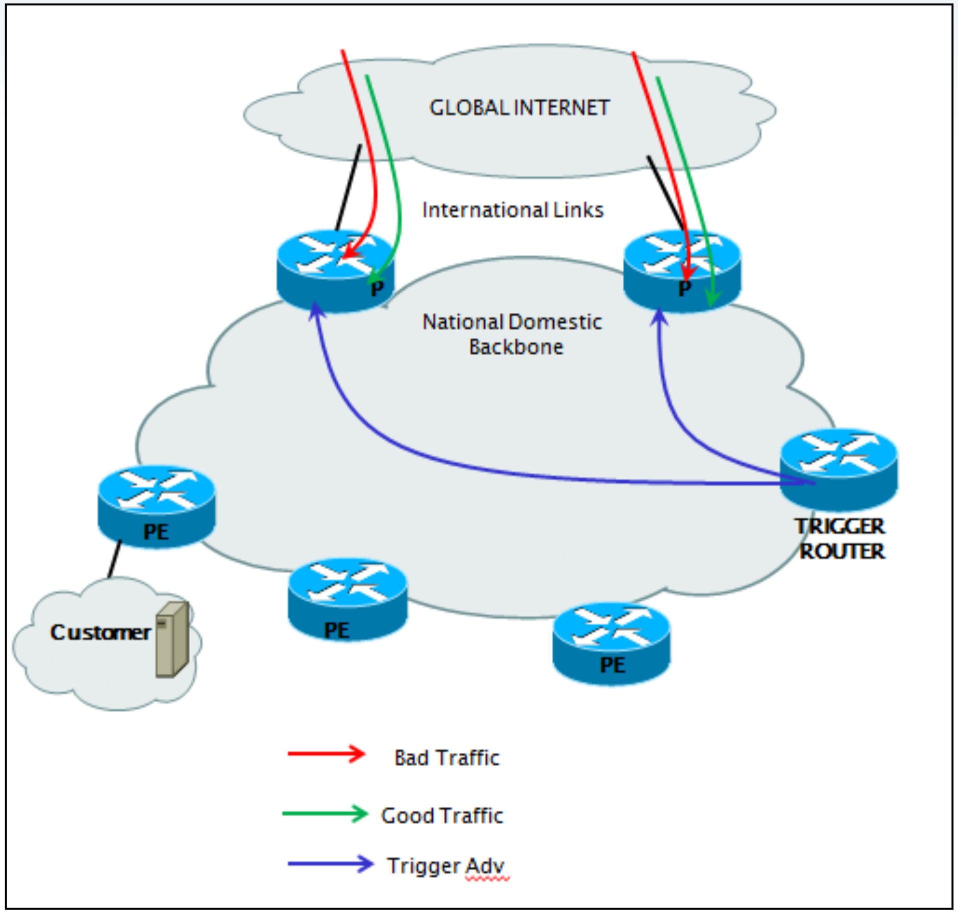
What is RTBH ?

- **Remote Triggered Black Hole** (RTBH), is a security **technique** where it requires sinking hole routers to drop the packets.
- There will be an advertising router, using **IBGP** Protocol that announces the route/IP to border routers (trigger).
- The border routers which are in transit paths receive DDOS packets and drop them using a reserved IP address (normally not public).

Sample flow of RTBH

Below is the sample flow of a **destination** based RTBH session.





Sample config of RTBH?

Below is the sample configuration of simple RTBH (Cisco) at the **Injector** router (**accessible inside NOC**) .

```
At Injector/Trigger router :
!
router ospf 100
log-adjacency-changes
redistribute connected subnets
network 192.168.4.0 0.0.0.255 area 0
!
router bgp 740
no synchronization
bgp log-neighbor-changes
redistribute static route-map black-hole-trigger
neighbor black-hole peer-group
neighbor black-hole remote-as 740
neighbor black-hole update-source Loopback0
neighbor black-hole send-community
neighbor 192.168.255.246 remote-as 740
neighbor 192.168.255.246 update-source Loopback0
neighbor 192.168.255.253 peer-group black-hole
no auto-summary
```

```
!
! Activation happens when an attack has been   !
identified.
ip route 61.6.16.135 255.255.255.255 Null0 tag 777
!
route-map black-hole-trigger permit 10
match tag 777
set ip next-hop 192.0.2.1 (reserved adress)
set local-preference 200
set origin igp
set community no-export
!
route-map black-hole-trigger deny 25
!
no scheduler allocate
end
```

Sample config of RTBH?

The trigger router: We can drop packets due to many reasons :

1) Router Advertises the /32 IP under attack into iBGP with. the “**777**” tag:

```
ip route 61.6.16.135 255.255.255.255 Null0 tag 777
```

2) Sink Hole Router advertising a large block of **un-allocated** address space (from IANA) with the BGP no-export community and BGP Egress route filters to keep the block inside.

```
ip route 96.0.0.0 224.0.0.0 Null0 tag 777
```

3) **Bogon** addresses (private+reserved addresses) to be dropped.

```
ip route 172.20.20.1 255.255.255.255 Null0 tag 777
ip route 10.0.0.0 255.0.0.0 Null0 tag 777
```

Destination based RTBH

Below is the sample configurations of **Destination** based RTBH technique on Border :

```
AT Border :

interface loopback0
ip address x.x.x.x 255.255.255.255
!
interface null0
no ip unreachables
!
router bgp 740
no synchronization
bgp log-neighbor-changes
neighbor black-hole peer-group
neighbor black-hole remote-as 65535
neighbor black-hole update-source loopback0
neighbor a.a.a.a peer-group black-hole
no auto-summary
!
ip route 192.0.2.1 255.255.255.255 null 0
```

Destination based RTBH

Sample verification of the iBGP advertisement :

AT Border :

```
BKJXX#sh ip bgp community no-export
BGP table version is 63, local router ID is XX.168.255.249
Status codes: s—suppressed, d—damped, h—history, * valid, > best, i—internal,
              r RIB-failure
Origin codes: i—IGP, e—EGP, ?—incomplete

Network              Next Hop    Metric LocPrf  Weight Path
*>i61.6.16.135./32   192.0.2.1   0         200  0       i
```

AT Border :

```
BGP updates debugging is on (inbound)
*Mar 1 22:26:27.750: BGP(0): 61.6.16.135 rcvd UPDATE w/ attr: nexthop 192.0.2.1, origin i,localpref 200, metric 0, community no-export
*Mar 1 22:26:27.754: BGP(0): 61.6.16.135 rcvd 192.168.1.100/32
*Mar 1 22:26:27.754: BGP(0): Revise route installing 1 of 1 route for 61.6.16.135 /32 -> 192.0.2.1 to main IP table
```

At Triggering Router :

If the attacks stop, need to remove the static router from Triggering router.

```
Black-hole# no ip route 61.6.16.135 255.255.255.255 null0 tag 777
```

Advanced RTBH : Source based

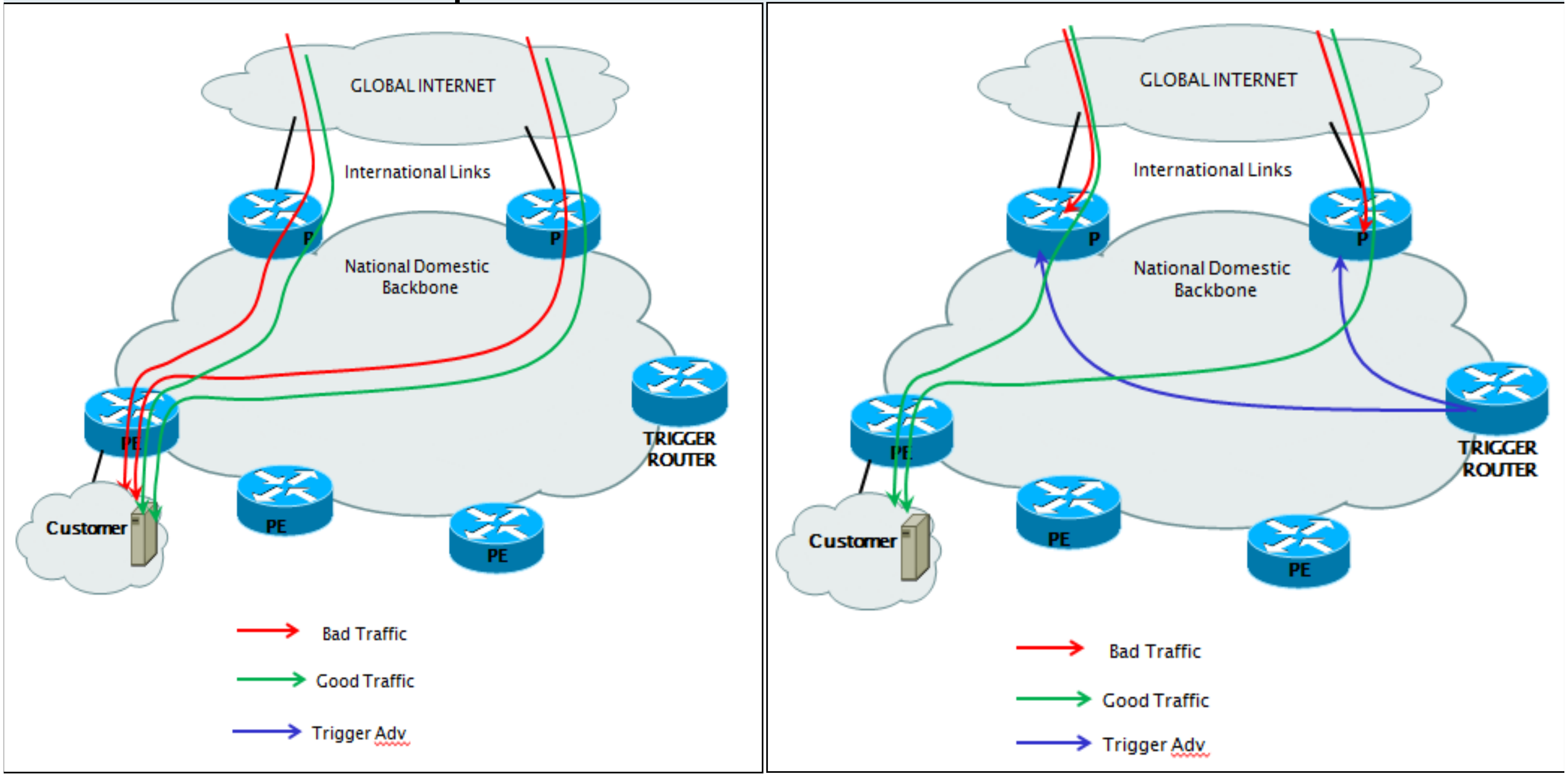
- Previous **destination** based technique is easy to setup by having one trigger router and deploy sinking configs at all border routers. However, it does not solve :
  - If the destination addresses are **enormous** which requires a high number of static routes.
  - **All traffic are dropped**, including legitimate traffic.

- Preferably, one way to solve this is to deploy **advanced Source** based technique which can cater for Source based requirement.

- With this, we can allow **legitimate traffic to pass through**, while customer server is "up".

Advanced RTBH : Source based

Below is the sample flow of **source** based RTBH session :

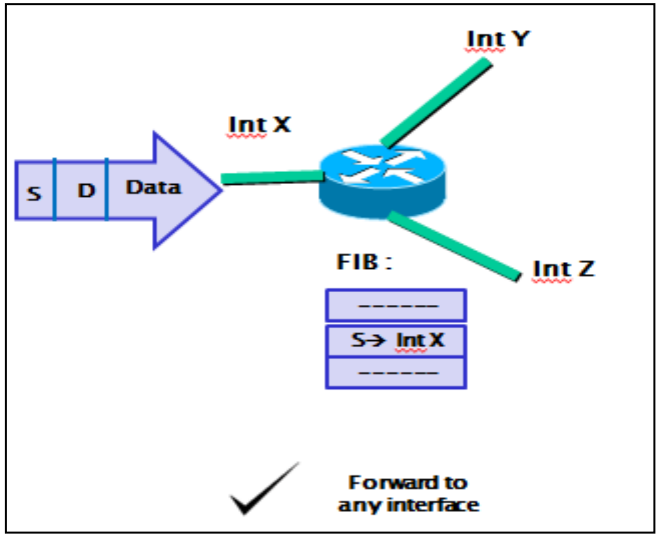


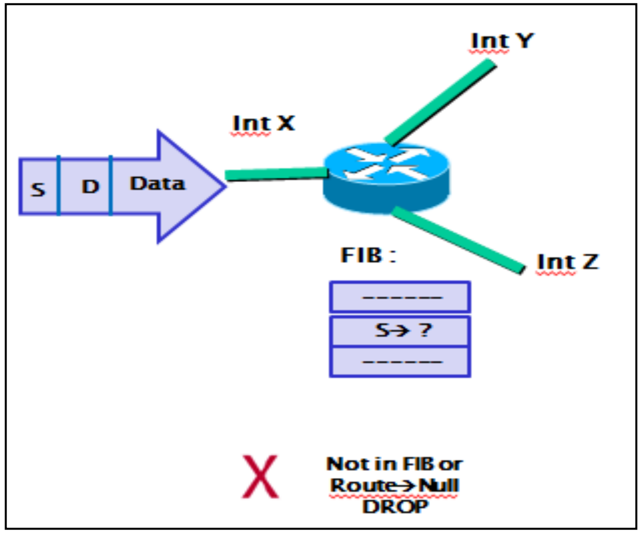
Advanced RTBH : Use URPF

Crossing borders. Changing lives.

Loose URPF : How does it work ?

- Implementation of source-based RTBH depends on loose mode Unicast Reverse Path Forwarding (URPF).
- Loose URPF checks the packet and forwards it if there is a route entry for the source IP of the incoming packet in the router FIB.
- In our RTBH case, the route **next hop is set to Null0**, the RPF check fails, and the packet is dropped as intended.





Advanced RTBH

- Below is the sample configuration of advance Source based RTBH technique (Cisco) at Border routers.

```
!
interface POS5/0/0
 description - link to Upstream-1
 ip address 172.16.100.9 255.255.255.252
 no ip redirects
 no ip directed-broadcasts
 ip verify unicast source reachable-via any
!
```

- If you believed that Unicast RPF is dropping packets that are deemed valid (false alarm), it may be necessary to configure an **access list (ACL)** within Unicast loose RPF. Be extra careful on the asymmetric nature of IP traffic.

```
!
interface POS4/0/0
 description - link to Upstream-2
 ip address 172.16.100.9 255.255.255.252
 ip verify unicast source reachable-via any 199
!
```

Agenda :

1) Refresher : Intro to DDOS
2) JARING's experience in early 2000
3) The use of RTBH : Simple vs Advanced
4) The end to end services (FW/QoS)
5) The deployment of DDOS Armour
6) The outcome ?

The end to end service

Having RTBH alone, is not enough to protect the customers and Infra :

- The whole IP/block is drop, even it is a business critical server that service Web sites, Emails, Online transaction, etc. The customers need to be **protected up to their premise** to defend service performance.

- The RTBH techniques, will heavily depend on **manual process** and **lacking SLA** components.

- The customer normally need some kind of **reporting documents** that can explain the attack behaviors and subsequently report to their management.

JARING
come together

The end to end service

Crossing borders. Changing lives.

JARING Introduced Unified Threat Mgmt (UTM+) service that complements the RTBH :

- It is a **managed Firewall** Security service from JARING that works together with Network Box (Hong Kong) and complements JARING SOC with 24 X 7 X 365 support.

- IPS/IDS with real time push updates, real time monitoring, load balancing and advanced reporting.

- **Basic DDOS prevention**, Anti-malware, Anti-Sypaware, Anti-Virus, Anti-Spam, VPN, Content Filtering, Web proxy.

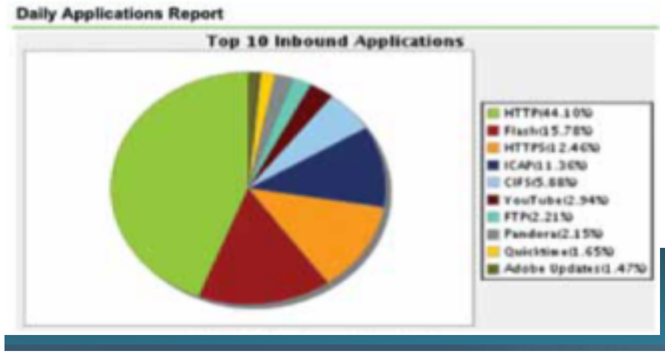
- Market differentiation : Multiple security blends that give real time, and Heuristic protection.

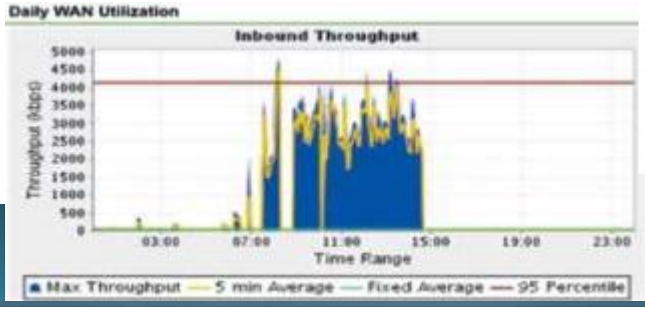
NETWORK BOX

The end to end service

The second complementary managed service is Unified Performance Mgmt (UPM) :

- Managed traffic optimization service. It is a QoS application service from Exinda that complements in **identifying the abnormal DDOS** traffic pattern.
- Bandwidth mgmt control, Traffic Shaping, Application acceleration, prioritization.
- Visibility, reporting of **top talkers**, Layer 7 application reports, proxy detection, real time monitoring.
- Market differentiation : Provide leading Unified Performance mgmt encompasses visibility, control and Optimization.





Agenda :

1) Refresher : Intro to DDOS
2) JARING's experience in early 2000
3) The use of RTBH : Simple vs Advanced
4) The end to end services (FW/QoS)
5) The deployment of DDOS Armour
6) The outcome ?

The deployment of DDOS Armour

- In year 2010, we embarked on the journey to have a better DDOS prevention system **mitigation** in place.

- We decided to go for Arbor Solution (www.arbornetworks.com) after evaluating the advanced features offered by the vendor.

- The system consists of CP and TMS devices :

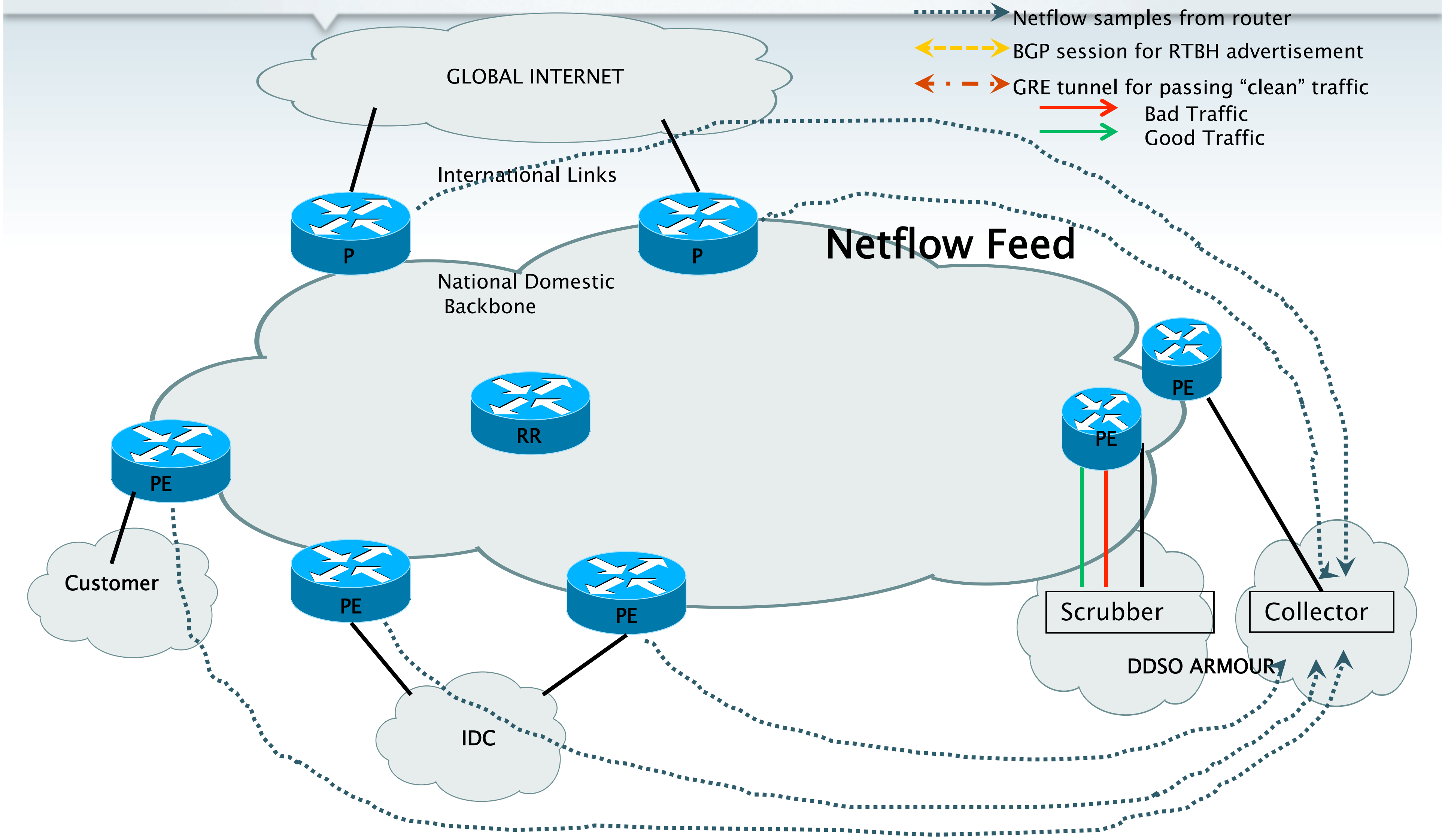
  - CP (**Collector** Platform) : Perform collection of Netflow info (layer , IP) and analyze and correlate the data from Border routers.

  - TMS (Threat Mgmt Service/**Scrubber**) : Perform Mitigation and BlackHole. Perform storing of temporary raw packets.

JARING DDoS Armour

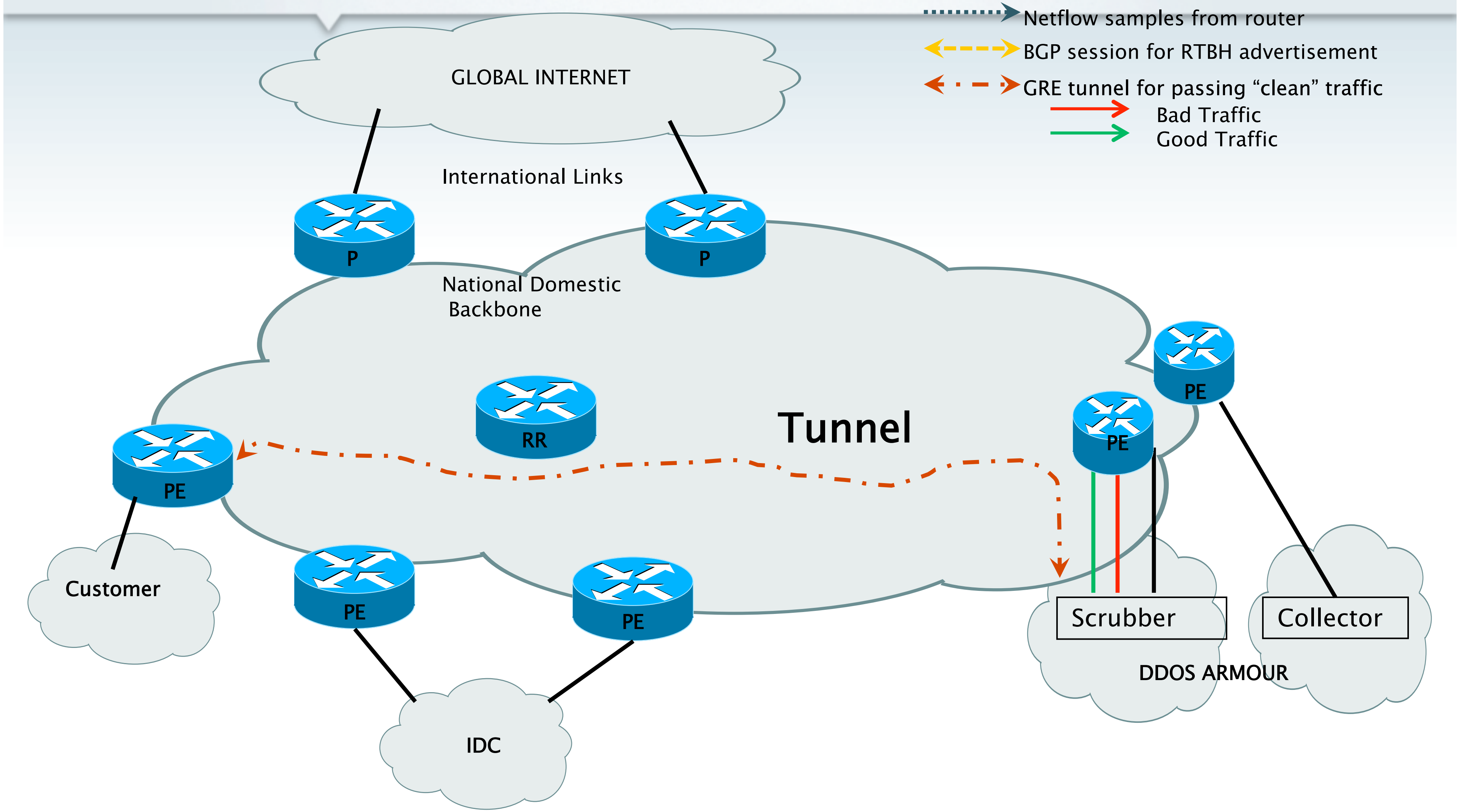
Helps Protect Your Business

How it works ? Netflow !!



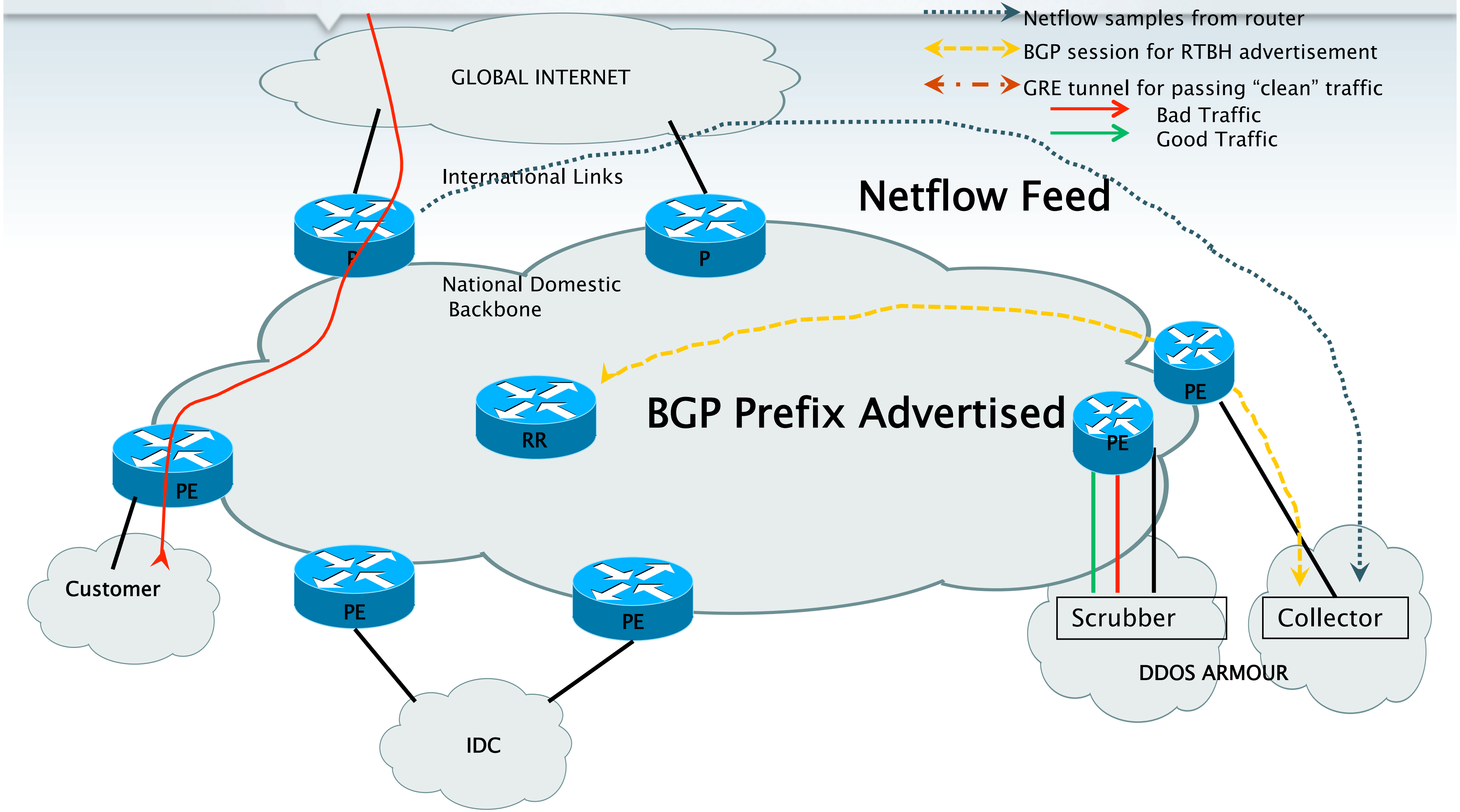
Netflow samples from router
BGP session for RTBH advertisement
GRE tunnel for passing “clean” traffic
Bad Traffic
Good Traffic
GLOBAL INTERNET
International Links
P
P
Netflow Feed
National Domestic Backbone
RR
PE
PE
PE
PE
PE
Customer
IDC
Scrubber
Collector
DDSO ARMOUR

How it works ? Tunnel !!

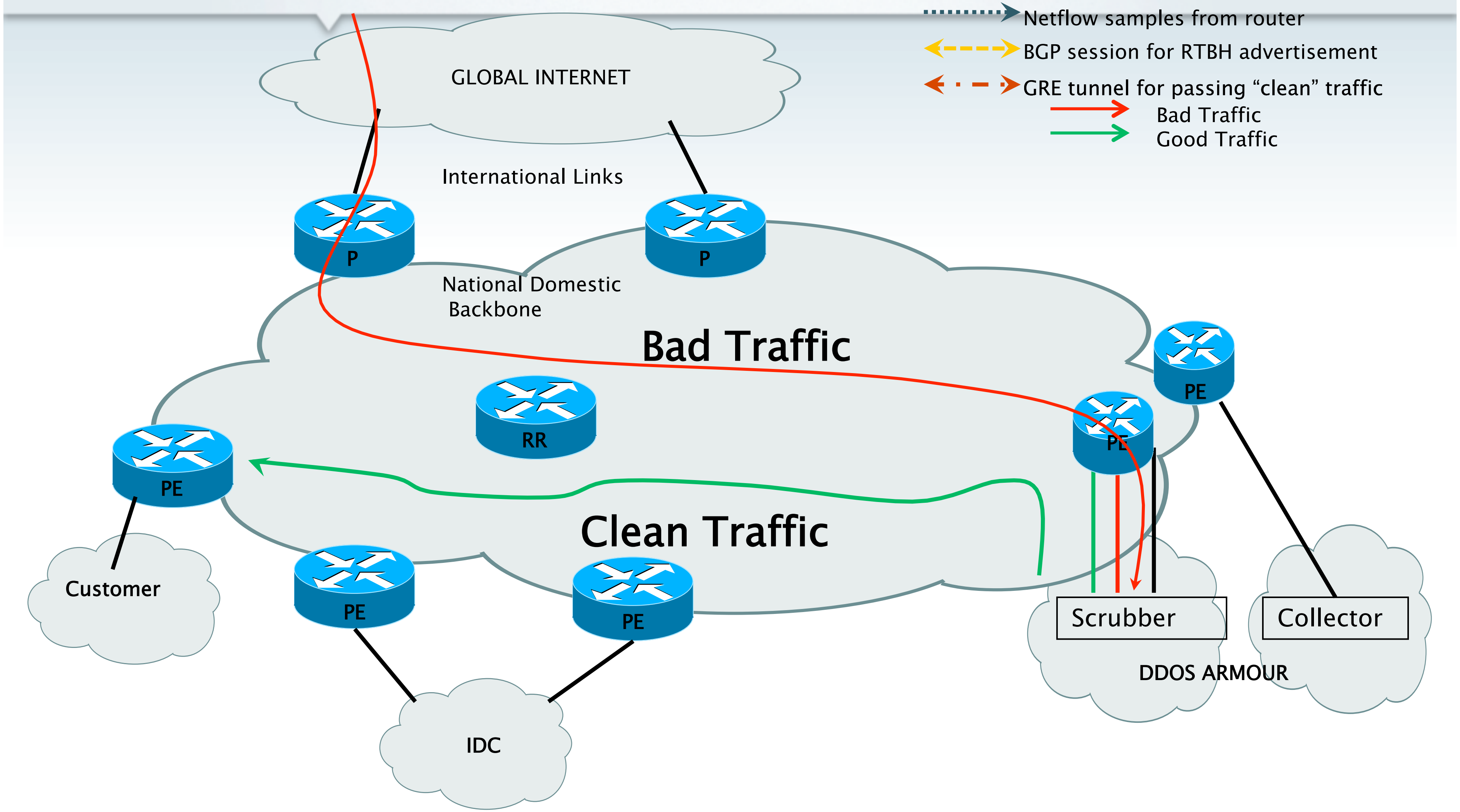


Netflow samples from router
BGP session for RTBH advertisement
GRE tunnel for passing "clean" traffic
Bad Traffic
Good Traffic
GLOBAL INTERNET
International Links
P
P
National Domestic Backbone
RR
Tunnel
PE
PE
PE
PE
PE
PE
Customer
IDC
Scrubber
Collector
DDOS ARMOUR

How it works ? Advertise !!



How it works ? Mitigate !!



Armour Basic Facts

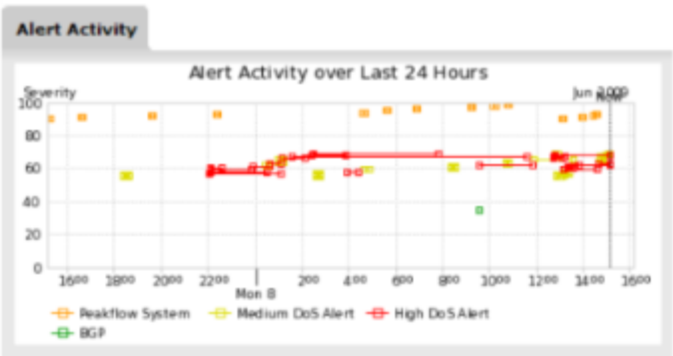
The system is designed to detect DDOS occurrences via 3 methods :

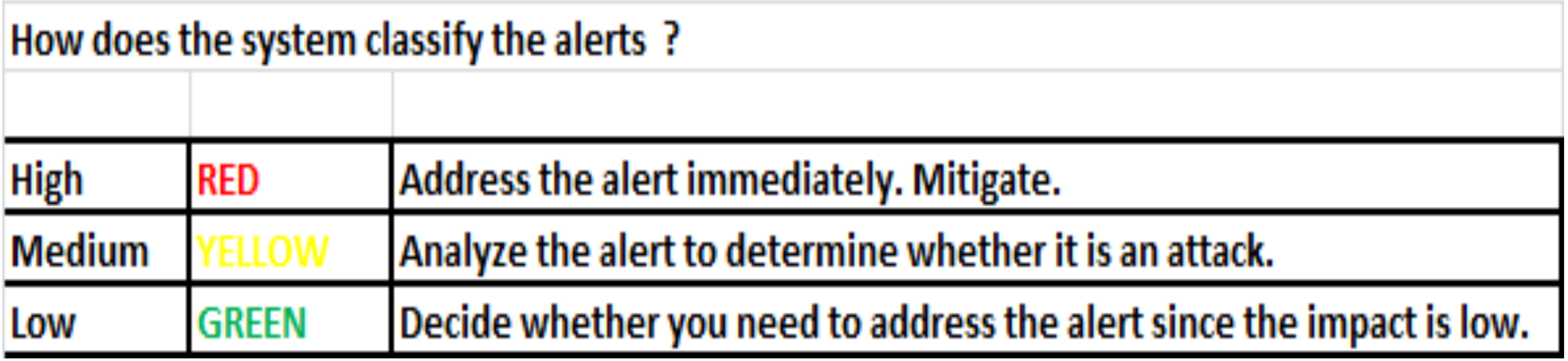
- **Misuse Anomaly** – deviate from normal Internet practices : tcp null,syn,rst, malformed packets attacks : IP fragment, smurf, fraggle, etc
- **Profile detection** – Deviation from normal traffic patterns/threshold.
- **FingerPrint Signatures** (Sharing among Arbor customer members) – new attacks with identified signatures.

Armour Basic Facts

There are 3 levels of severity defined by the system :

- ○ High
- ○ Medium
- ○ Low





How does the system classify the alerts ?

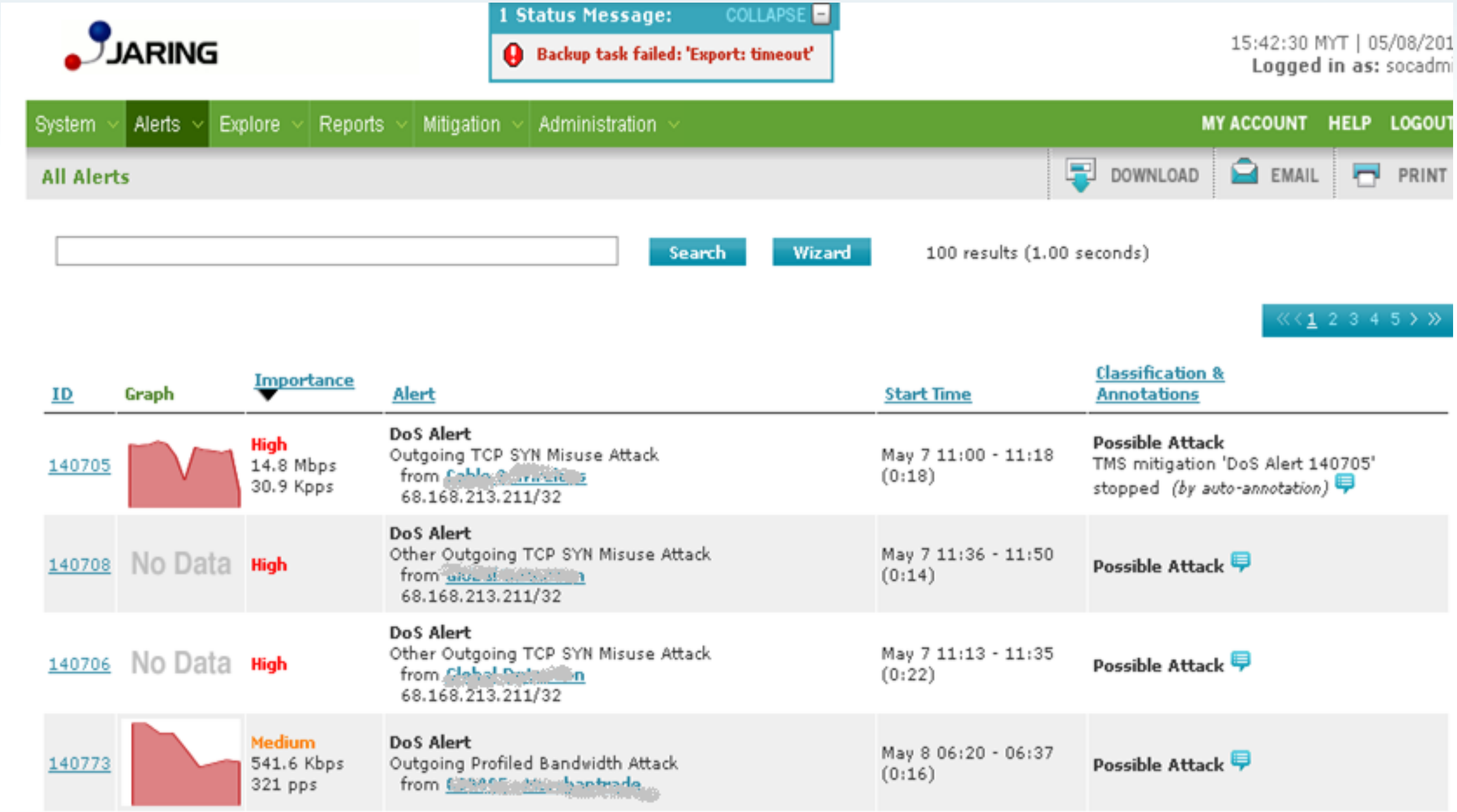
High	RED	Address the alert immediately. Mitigate.
Medium	YELLOW	Analyze the alert to determine whether it is an attack.
Low	GREEN	Decide whether you need to address the alert since the impact is low.

JARING come together

Armour Basic Facts

Crossing borders. Changing lives.

Sample dashboard report for customer :



JARING

1 Status Message: COLLAPSE

Backup task failed: 'Export: timeout'

15:42:30 MYT | 05/08/201

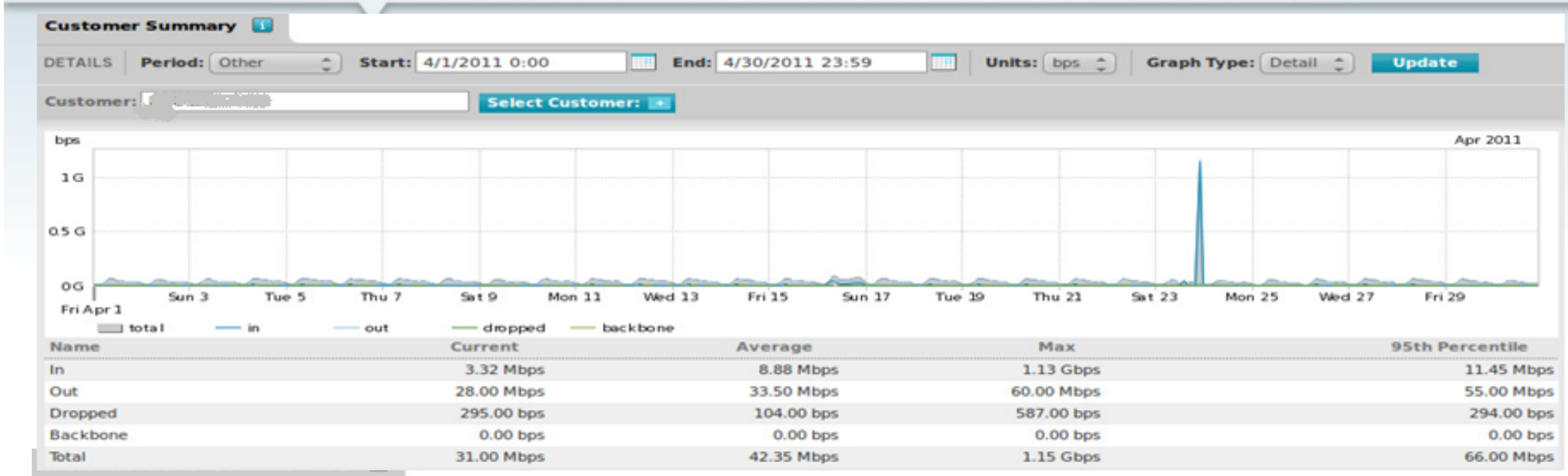
Logged in as: socadmi

All Alerts

100 results (1.00 seconds)

ID	Graph	Importance	Alert	Start Time	Classification & Annotations
140705		High 14.8 Mbps 30.9 Kpps	DoS Alert Outgoing TCP SYN Misuse Attack from [redacted] 68.168.213.211/32	May 7 11:00 - 11:18 (0:18)	Possible Attack TMS mitigation 'DoS Alert 140705' stopped *(by auto-annotation)*
140708	No Data	High	DoS Alert Other Outgoing TCP SYN Misuse Attack from [redacted] 68.168.213.211/32	May 7 11:36 - 11:50 (0:14)	Possible Attack
140706	No Data	High	DoS Alert Other Outgoing TCP SYN Misuse Attack from [redacted] 68.168.213.211/32	May 7 11:13 - 11:35 (0:22)	Possible Attack
140773		Medium 541.6 Kbps 321 pps	DoS Alert Outgoing Profiled Bandwidth Attack from [redacted]	May 8 06:20 - 06:37 (0:16)	Possible Attack

Armour : Sample Report

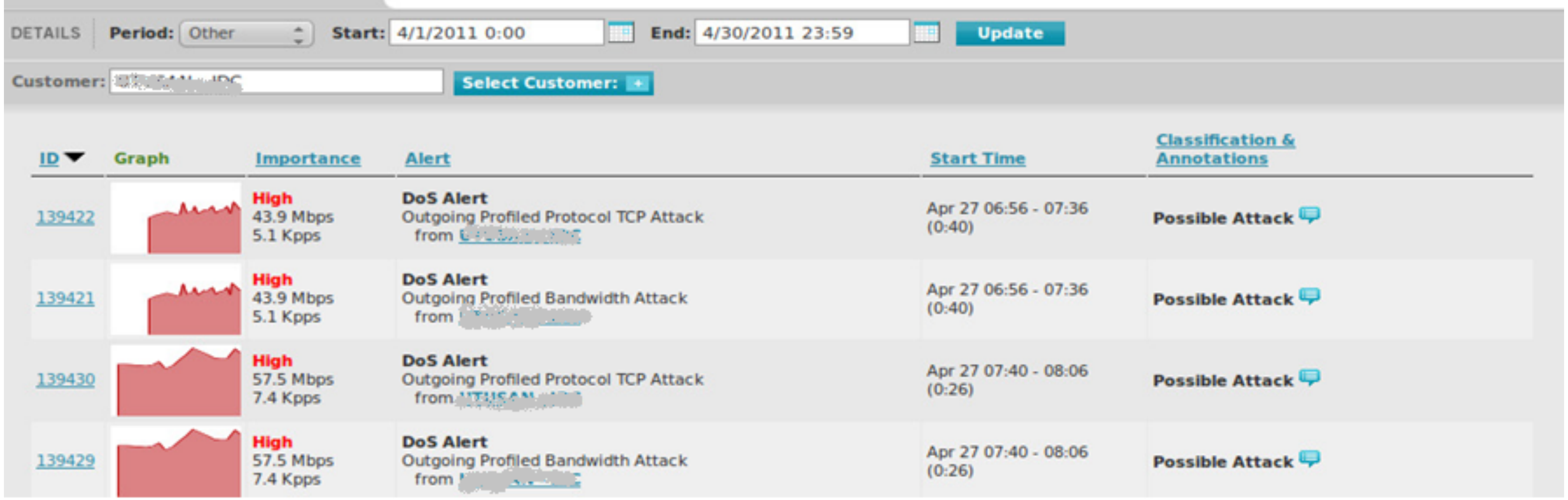


Customer Summary

DETAILS **Period:** Other **Start:** 4/1/2011 0:00 **End:** 4/30/2011 23:59 **Units:** bps **Graph Type:** Detail Update

Customer: [redacted] Select Customer:

Name	Current	Average	Max	95th Percentile
In	3.32 Mbps	8.88 Mbps	1.13 Gbps	11.45 Mbps
Out	28.00 Mbps	33.50 Mbps	60.00 Mbps	55.00 Mbps
Dropped	295.00 bps	104.00 bps	587.00 bps	294.00 bps
Backbone	0.00 bps	0.00 bps	0.00 bps	0.00 bps
Total	31.00 Mbps	42.35 Mbps	1.15 Gbps	66.00 Mbps



DETAILS **Period:** Other **Start:** 4/1/2011 0:00 **End:** 4/30/2011 23:59 Update

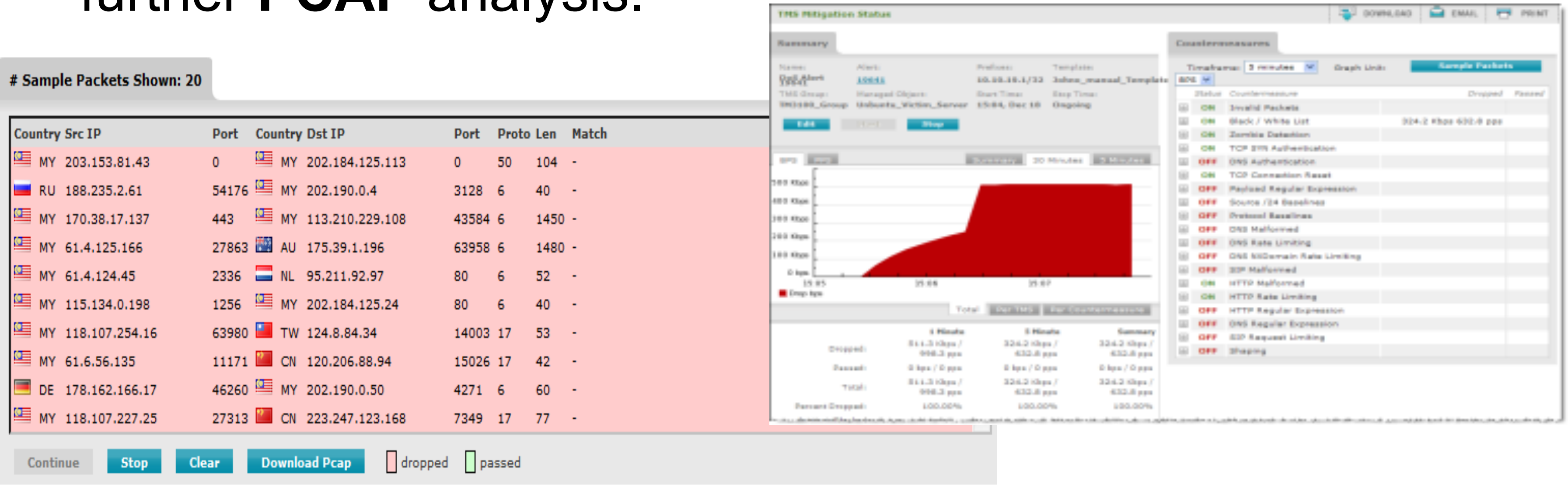
Customer: [redacted] Select Customer:

ID	Graph	Importance	Alert	Start Time	Classification & Annotations
139422		High 43.9 Mbps 5.1 Kpps	**DoS Alert** Outgoing Profiled Protocol TCP Attack from [redacted]	Apr 27 06:56 - 07:36 (0:40)	**Possible Attack**
139421		High 43.9 Mbps 5.1 Kpps	**DoS Alert** Outgoing Profiled Bandwidth Attack from [redacted]	Apr 27 06:56 - 07:36 (0:40)	**Possible Attack**
139430		High 57.5 Mbps 7.4 Kpps	**DoS Alert** Outgoing Profiled Protocol TCP Attack from [redacted]	Apr 27 07:40 - 08:06 (0:26)	**Possible Attack**
139429		High 57.5 Mbps 7.4 Kpps	**DoS Alert** Outgoing Profiled Bandwidth Attack from [redacted]	Apr 27 07:40 - 08:06 (0:26)	**Possible Attack**

Armour Basic Facts

- Traffic profiling data is stored in the local system. Furthermore, we **backup** the copy of the data in DRC offline storage (for permanent).

- The **packet sniffing** can be viewed during the attacks, if we want to check for signatures, attack pattern etc for further **PCAP** analysis.



# Sample Packets Shown: 20

Country	Src IP	Port	Country	Dst IP	Port	Proto	Len	Match
MY	203.153.81.43	0	MY	202.184.125.113	0	50	104	-
RU	188.235.2.61	54176	MY	202.190.0.4	3128	6	40	-
MY	170.38.17.137	443	MY	113.210.229.108	43584	6	1450	-
MY	61.4.125.166	27863	AU	175.39.1.196	63958	6	1480	-
MY	61.4.124.45	2336	NL	95.211.92.97	80	6	52	-
MY	115.134.0.198	1256	MY	202.184.125.24	80	6	40	-
MY	118.107.254.16	63980	TW	124.8.84.34	14003	17	53	-
MY	61.6.56.135	11171	CN	120.206.88.94	15026	17	42	-
DE	178.162.166.17	46260	MY	202.190.0.50	4271	6	60	-
MY	118.107.227.25	27313	CN	223.247.123.168	7349	17	77	-

□ dropped □ passed

TMS Mitigation Status

Summary

Name: DoS Alert 19841
Alert: 19841
Prefixes: 10.10.10.1/32
Template: Johns_manual_Template
TMS Group: TMS100_Group
Managed Object: Ubuntu_Victim_Server
Start Time: 15:04, Dec 10
Stop Time: Ongoing

	1 Minute	5 Minute	Summary
Dropped:	811.3 Kbps / 998.3 pps	324.2 Kbps / 632.8 pps	324.2 Kbps / 632.8 pps
Passed:	0 bps / 0 pps	0 bps / 0 pps	0 bps / 0 pps
Total:	811.3 Kbps / 998.3 pps	324.2 Kbps / 632.8 pps	324.2 Kbps / 632.8 pps
Percent Dropped:	100.00%	100.00%	100.00%

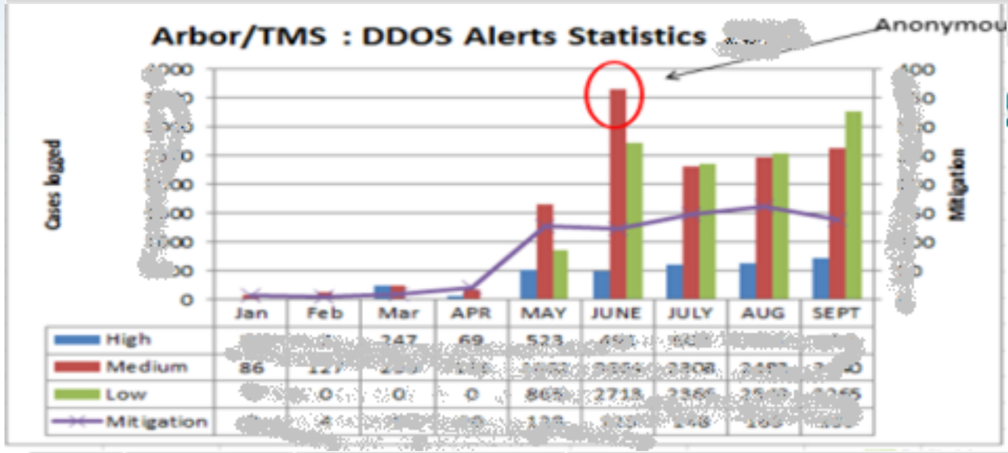
Countermeasures

Timeframe: 5 minutes Graph Unit: BPS

Status	Countermeasure	Dropped	Passed
ON	Invalid Packets		
ON	Black / White List	324.2 Kbps 632.8 pps	
ON	Zombie Detection		
ON	TCP SYN Authentication		
OFF	DNS Authentication		
ON	TCP Connection Reset		
OFF	Payload Regular Expression		
OFF	Source /24 Baselines		
OFF	Protocol Baselines		
OFF	DNS Malformed		
OFF	DNS Rate Limiting		
OFF	DNS NXDomain Rate Limiting		
OFF	SIP Malformed		
ON	HTTP Malformed		
ON	HTTP Rate Limiting		
OFF	HTTP Regular Expression		
OFF	DNS Regular Expression		
OFF	SIP Request Limiting		
OFF	Shaping		

Sample Stats

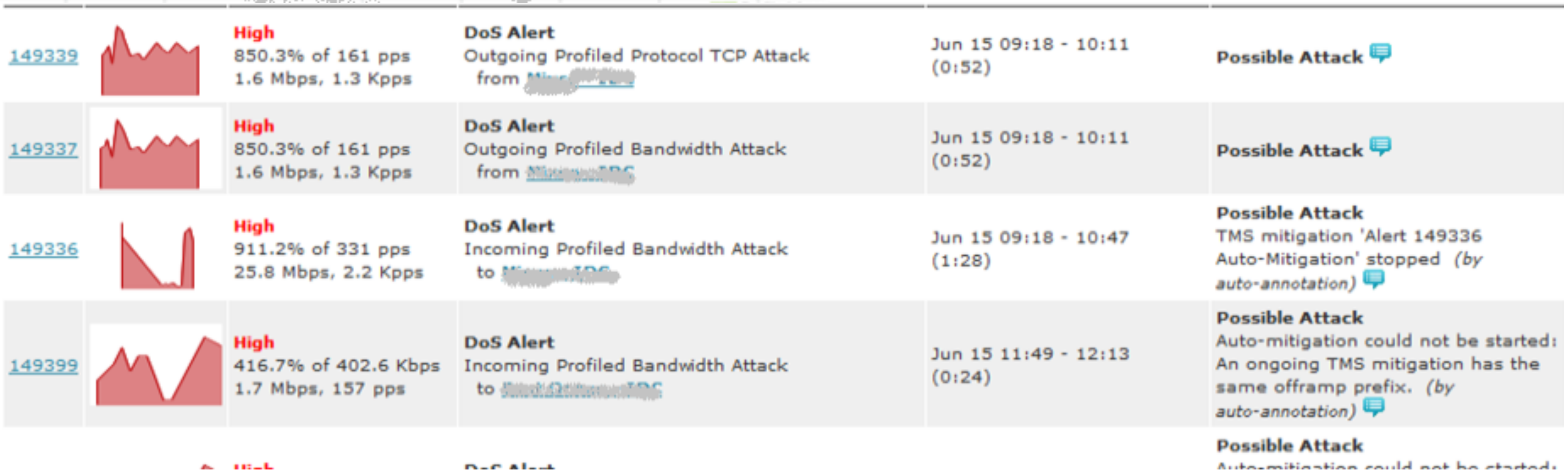
- There are many "high" category during the 1st week of the "**anonymous army attack**" starting June 15-22, 2011.



Arbor/TMS : DDOS Alerts Statistics [redacted]

	Jan	Feb	Mar	APR	MAY	JUNE	JULY	AUG	SEPT
🟦 High	[redacted]	[redacted]	247	69	523	[redacted]	[redacted]	[redacted]	[redacted]
🟥 Medium	86	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2308	[redacted]	[redacted]
🟩 Low	[redacted]	[redacted]	[redacted]	0	865	2718	[redacted]	[redacted]	[redacted]
Mitigation	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

IRC.ANONOPS.LI
#OPMALAYSIA
PORT: 6667
Wednesday,
June 15
7:30 PM
GMT
Operation Malaysia
TARGET: HTTP://WWW.MALAYSIA.GOV.MY
OPERATION MALAYSIA



rch Wizard 116 res

				Start Time ▲	Classification & Annotations
149339		**High** 850.3% of 161 pps 1.6 Mbps, 1.3 Kpps	**DoS Alert** Outgoing Profiled Protocol TCP Attack from [redacted]	Jun 15 09:18 - 10:11 (0:52)	**Possible Attack**
149337		**High** 850.3% of 161 pps 1.6 Mbps, 1.3 Kpps	**DoS Alert** Outgoing Profiled Bandwidth Attack from [redacted]	Jun 15 09:18 - 10:11 (0:52)	**Possible Attack**
149336		**High** 911.2% of 331 pps 25.8 Mbps, 2.2 Kpps	**DoS Alert** Incoming Profiled Bandwidth Attack to [redacted]	Jun 15 09:18 - 10:47 (1:28)	**Possible Attack** TMS mitigation 'Alert 149336 Auto-Mitigation' stopped *(by auto-annotation)*
149399		**High** 416.7% of 402.6 Kbps 1.7 Mbps, 157 pps	**DoS Alert** Incoming Profiled Bandwidth Attack to [redacted]	Jun 15 11:49 - 12:13 (0:24)	**Possible Attack** Auto-mitigation could not be started: An ongoing TMS mitigation has the same offramp prefix. *(by auto-annotation)*
		High	**DoS Alert**		**Possible Attack** Auto-mitigation could not be started:

Agenda :

1) Refresher : Intro to DDOS
2) JARING's experience in early 2000
3) The use of RTBH : Simple vs Advanced
4) The end to end services (FW/QoS)
5) The deployment of DDOS Armour
6) The outcome ?

The outcome ?

- With Armour, JARING has added a valuable tool that benefits the Infrastructure :
  - By avoiding the **potential loss of SLA** from DDOS attacks, it improves image of the Service Provider (SP) to their customers, and promotes customer retention.
  - JARING has the ability to view network activities relating to DDOS and **gather statistics and patterns**.
  - Has the ability to use the **BGP analysis tool** offered by Arbor on the stability of BGP Infra.
  - Has the ability to use **geo-location & peering tools,** to determine the best peering partners. To gauge other stats, such as average/common MTU, etc.

The outcome ?

- Benefits to the customer :
  - The customer can **be protected** and it ensures business continuity is at the higher level and protects their service reputation.
  - The mitigation is **real time and this proactive** monitoring (instead of reactive) and mitigation help to defer attack pattern of either sudden high traffic or prolong interval of attacks.
  - Customer is **off loaded from fault resolution process** of identifying the source/destination of the attacks (24 X 7 NOC). Without it, fault resolution process can consume Engineer’s valuable time.
  - Customer can view their traffic profile on **periodic reports** to check the current traffic pattern (**type, size, origin**) and also the historical DDOS occurrences.

Summary

- Service Providers (SP) **can't run away** from DDOS problems !!
- It consumes precious resource from your infrastructure as well as affecting customer's valuable service.
  - JARING used to rely on **Netflow and ACL/policy-map** pre year 2000.
  - Implemented **RTBH solution** as early as 2004.
  - **F/W and QOS** products have been introduced to complement the RTBH to reduce the impact of DDOS up to customer's place.
  - In 2010, JARING has successfully deployed Armour system **with mitigation (scrubber)** to protect Infra/customers from outages due to DDOS attacks effectively.

References:

- Arbor Solution : www.arbor.net
- Network Box : www.network-box.com
- Exinda (QOS) : www.exinda.com
- Cisco Website : www.cisco.com
- JARING Products : www.jaring.my

- DDOS resources on WEB :
  - www.**ddos**info.com
  - www.denial-of-service-attack.com/
  - www.ddosinfo.com/

JARING
come together

Crossing borders. Changing lives.

Thank You

Managing DDOS: JARING’s DDOS Experience

zamzuri@jaring.my

CERTIFIED TO ISO/IEC 27001:2005
CERT. NO. : AR 5438

CERTIFIED TO ISO 9001:2008
CERT. NO. : AR 5437

CERTIFIED TO ISO 9001:2008
CERT. NO. : AR 5437

THE INTERNATIONAL
CUSTOMER SERVICE INSTITUTE

OPEN DATA CENTER ALLIANCE
MEMBER