IPSERVERONE®

DDOS MITIGATION EXPERIENCE

01.

About
IP ServerOne

IP SERVER ONE
Trusted . Reliable . Secured Hosting Provider

About IP ServerOne

- Founded in **2003**
- **52** Employees
- Managing over 4500 physical servers
- Total **150** Racks in **5** data centers across **Malaysia and Singapore**
- Contributing **10%** of Malaysia's domestic traffic
- Approximately **6.8 Gbit/s** total traffic sending to the Internet at peak
- **300 Gbps** DDoS mitigation capacity in **MY, SG, HK, TW**

02.

What is **a** **DDoS attack?**

IPSERVERONE®
Trusted . Reliable . Secured Hosting Provider

Why choosing this topic?

01 · We believe that everyone should be more aware of DDoS attacks and their **possible impacts on a business**

02 · To share on the **DDoS trend happening in our local community**

03 · To share the possible ways to **detect any kind of DDoS attack**, and help to blackhole the affected IP addresses automatically with opensource utility

04 · Giving an idea of **IPSERVERONE's anti-ddos system deployment** in our own data centers

A cyberattack carried out over networks that intentionally is done by someone

In short, it's
a downtime to the provider

Or

a downtime to the customer

What is the level of attacks we encounter?

2-5 attacks per day

Over **100 attacks** per month

Mostly range from **4.5 Gbps** to **8.9 Gbps**

Attacks mainly come from **overseas**

Which types of attack we mostly get?

- **UDP floods**
- **TCP Flag floods** (SYN, ACK…)
- **HTTP/ HTTPS flood**
- **DNS/ NTP/ SSDP/ CHARGEN** amplification attack

Attacks from international link:

Bandwidth level attack:

International link is around 81 Gbit/s

Packet per second (pps) attack:

16.6 Mbps, bandwidth is approximately 6.6 Gbps

Attacks from Malaysia's peering

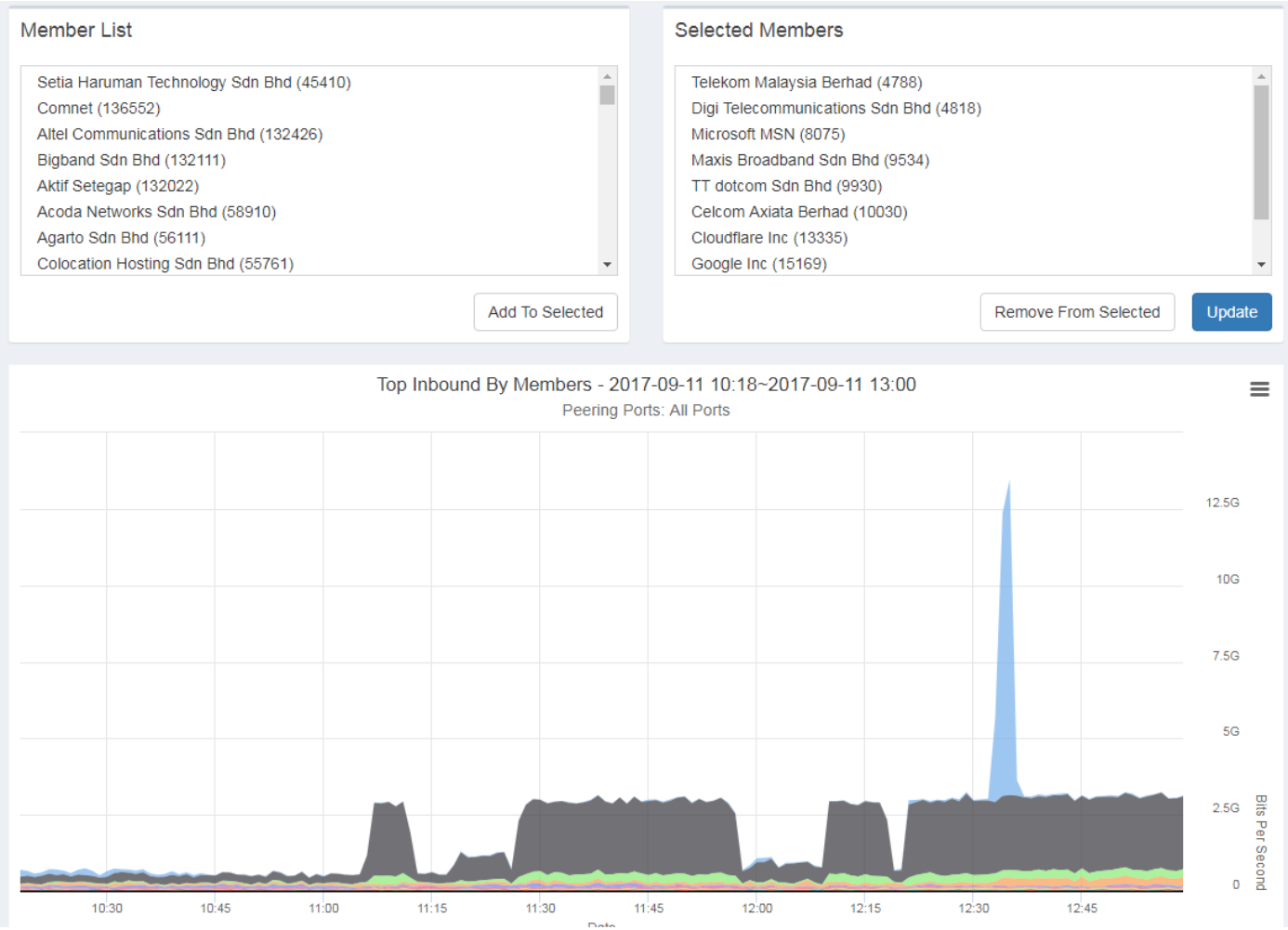
Bandwidth level attack:

12 Gbps from single provider

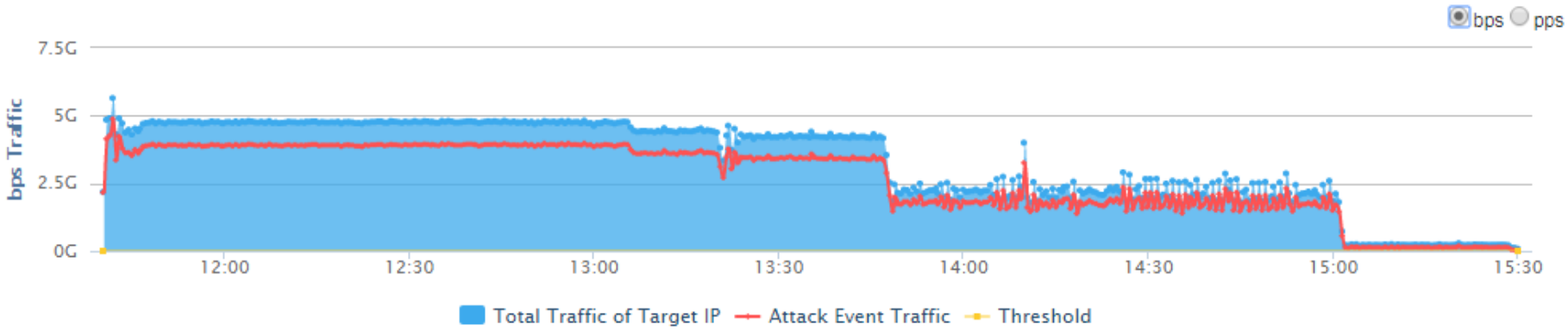
Packet per second (pps) attack:

10.6 Mbps, bandwidth is approximately 4.9 Gbps

DDoS activity within Malaysia

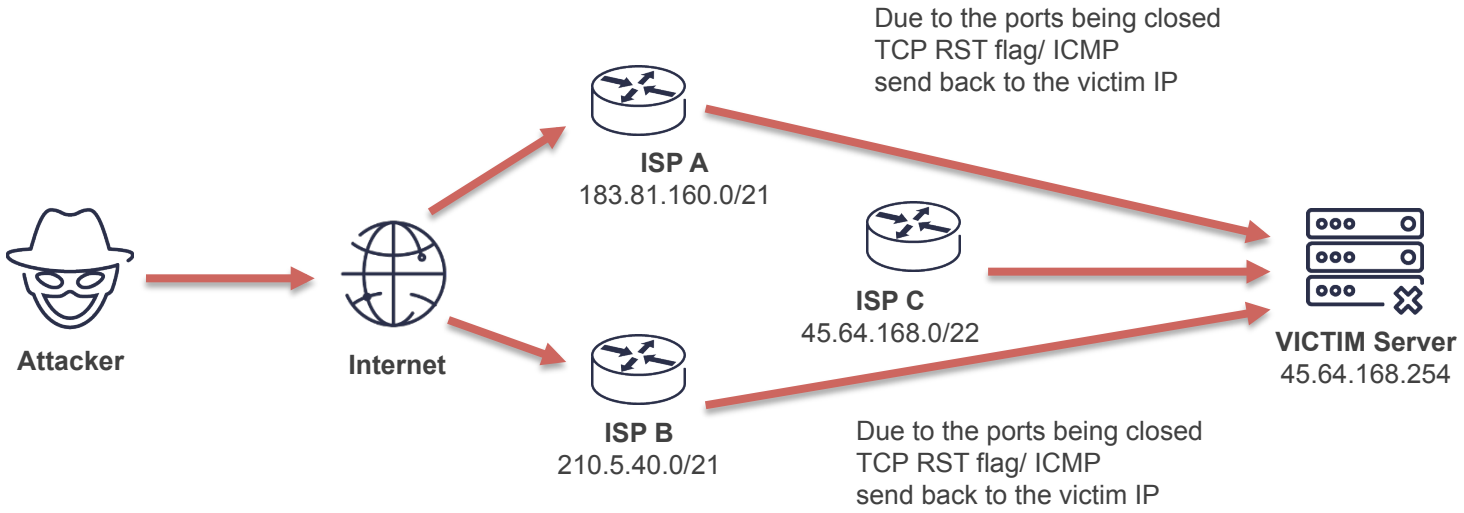


A DDoS alert report sample on a local attack



Maximum		Average		Current	
bps	pps	bps	pps	bps	pps
4.9G	10.6M	2.7G	5.8M	-	-

A new way of DDoS attack (via Direct Peering)



Spoofed IP **Source:** 45.64.168.254:80

Destination: 210.5.40.0 – 210.5.47.254 *(all ISP **B** IP addresses)*

Destination: 183.81.160.0 – 183.81.167.254 *(all ISP **A** IP addresses)*

Destination Port: 80,443,22,21…. **TCP Flag: SYN**

IPSERVERONE®
Trusted . Reliable . Secured Hosting Provider

The impacts from this new method attack:

01

- The attacker can control how to flow **the attack to the victim network**; For example: Via MyIX? Or direct peering & etc.

02

- The ISP A, or ISP B think that the victim server **is attacking all their IP address range**.

03

- **ISP A, or ISP B will not be able to do any blackhole** as all of their IP addresses are affected.

04

- **Victim ISP cannot react to it** as the packet was spoofed from outside of the victim network.

Solutions for these kind of attacks:

Make sure you **have enough bandwidth to take the spoofed packet**

Apply ACL, or using Flowspec to **mitigate this issue**

To sleep better

DDoS detection tool must be available

To do tcpdump / nfdump when you are under-attack it's way too slow

A Dedicated Blackhole router that integrates with ExaBGP can make the NOCs' lives easier

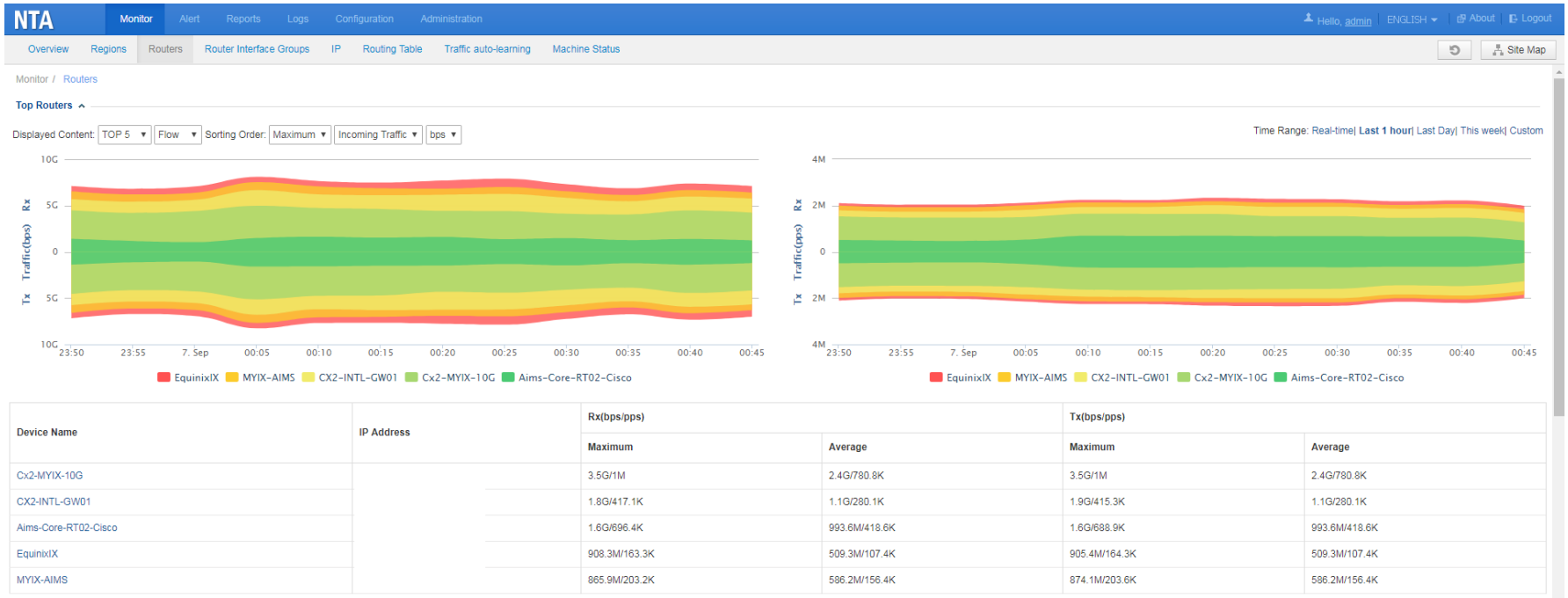
03.

How do we **detect a DDoS attack?**

IPSERVERONE
Trusted . Reliable . Secured Hosting Provider

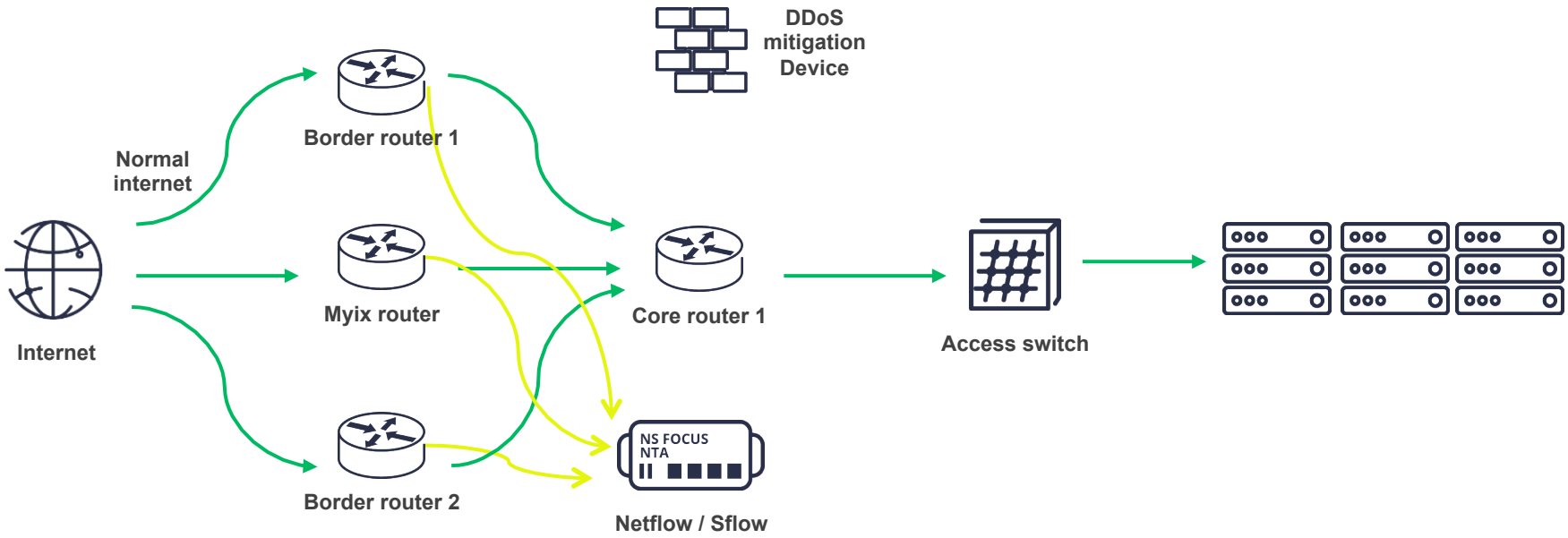
How do we detect a DDoS attack:

We use **netflow** to detect any kind of DDoS attack



Device Name	IP Address	Rx(bps/pps)		Tx(bps/pps)	
		Maximum	Average	Maximum	Average
Cx2-MYIX-10G		3.5G/1M	2.4G/780.8K	3.5G/1M	2.4G/780.8K
CX2-INTL-GW01		1.8G/417.1K	1.1G/280.1K	1.9G/415.3K	1.1G/280.1K
Aims-Core-RT02-Cisco		1.6G/696.4K	993.6M/418.6K	1.6G/688.9K	993.6M/418.6K
EquinixIX		908.3M/163.3K	509.3M/107.4K	905.4M/164.3K	509.3M/107.4K
MYIX-AIMS		865.9M/203.2K	586.2M/156.4K	874.1M/203.6K	586.2M/156.4K

Detector deployment architecture



1. We use **out of path deployment**
2. **NTA** will collect flow from all the border routers
3. Traffic will pass through normally from:

   border > core router > access > switch > server

How does a detector work?

The detector will look at the **netflow packet** and will count for **the number of packet per seconds** towards single destination IP address.

In layman term, it will count how many:

1. SYN packet received per second for single IP
2. ACK packet received per second for single IP
3. DNS packet received per second for single IP
4. NTP packet received per second for single IP
5. UDP packet received per second for single IP
6. ..... (and many many more)

Detector Threshold setting

We categorize all our IP addresses into Multiple IP address groups

Alert Type	Detect Mode *	Threshold (bps/pps)		Alert Hierarchy (%)		Diversion Level
		Latent Alert Threshold	Direct Alert Threshold	Medium	High	
SYN FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
ACK FLOOD	Packets only	0/20.0K	0/40.0K	150	200	Divert Traffic of Low-level Alert
UDP FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
ICMP FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
IGMP FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
PROTOCOL NULL FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
TCPFLAG MISUSE FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
TCPFLAG NULL FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
HTTP flood	Packets only	0/100.0K	0/200.0K	150	200	Divert Traffic of Low-level Alert
HTTPS FLOOD	Packets only	0/100.0K	0/200.0K	150	200	Divert Traffic of Low-level Alert
DNS REQUEST FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
DNS RESPONSE FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
LAND FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
SIP FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
DARK IP ABNORMAL	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
PRIVATE IP ABNORMAL	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
NTP REFLECTION FLOOD	Packets only	0/20.0K	0/40.0K	150	200	Divert Traffic of Low-level Alert
SSDP REFLECTION	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert

Each IP Group would contain its own IP range and threshold setting

DDoS detector also detects based on bandwidth

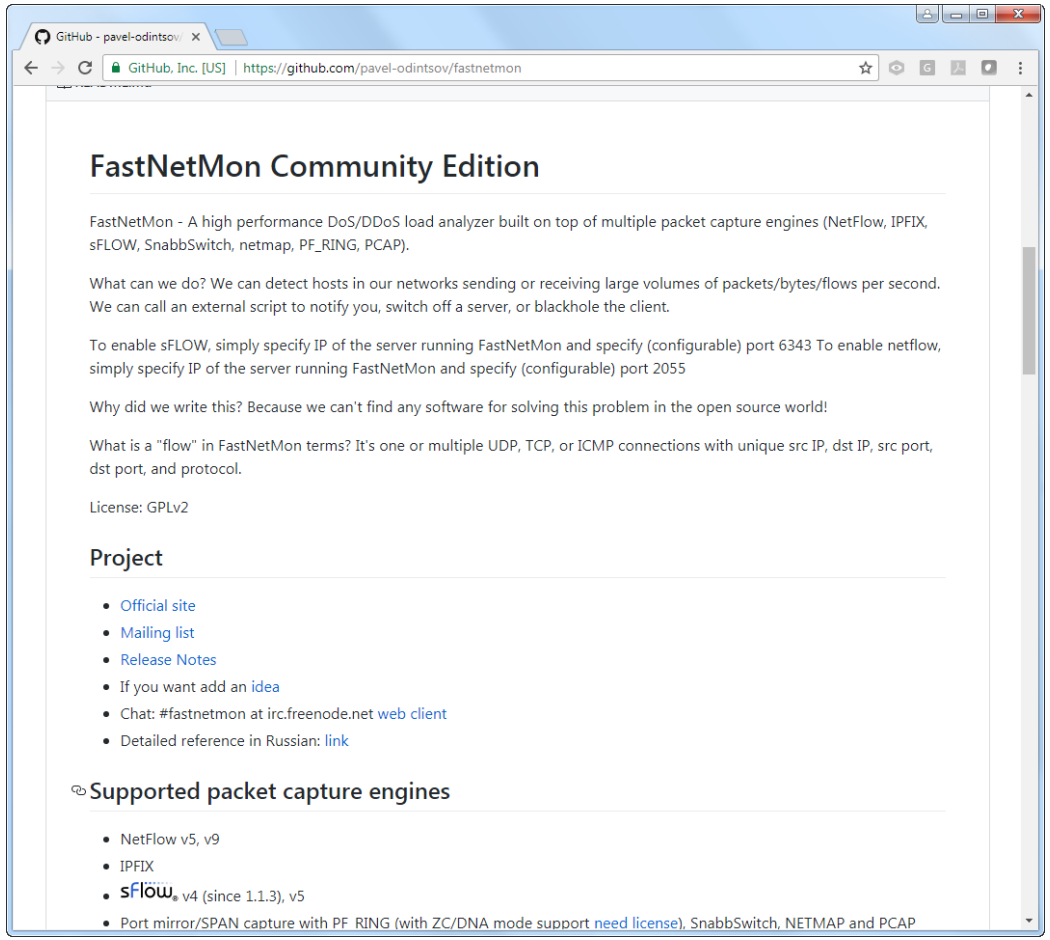
Besides Packet Per second check, it will also check for:
maximum inbound bandwidth per second for single IP

NTA | Monitor | Alert | Reports | Logs | Configuration | Administration

Objects | Alert Configuration Template | Global Alert Settings | Global Divert Settings | Flow Settings | Data Dictionary

TCPFLAG MISUSE FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
TCPFLAG NULL FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
HTTP flood	Packets only	0/100.0K	0/200.0K	150	200	Divert Traffic of Low-level Alert
HTTPS FLOOD	Packets only	0/100.0K	0/200.0K	150	200	Divert Traffic of Low-level Alert
DNS REQUEST FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
DNS RESPONSE FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
LAND FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
SIP FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
DARK IP ABNORMAL	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
PRIVATE IP ABNORMAL	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
NTP REFLECTION FLOOD	Packets only	0/20.0K	0/40.0K	150	200	Divert Traffic of Low-level Alert
SSDP REFLECTION FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
SNMP REFLECTION FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
CHARGEN REFLECTION FLOOD	Packets only	0/10.0K	0/20.0K	150	200	Divert Traffic of Low-level Alert
TRAFFIC ABNORMAL	Bytes only	150.0M/0	200.0M/0	150	200	Divert Traffic of Low-level Alert

Open-source utility that can do a DDoS Detection:



GitHub - pavel-odintsov

GitHub, Inc. [US] | https://github.com/pavel-odintsov/fastnetmon

FastNetMon Community Edition

FastNetMon - A high performance DoS/DDoS load analyzer built on top of multiple packet capture engines (NetFlow, IPFIX, sFLOW, SnabbSwitch, netmap, PF_RING, PCAP).

What can we do? We can detect hosts in our networks sending or receiving large volumes of packets/bytes/flows per second. We can call an external script to notify you, switch off a server, or blackhole the client.

To enable sFLOW, simply specify IP of the server running FastNetMon and specify (configurable) port 6343 To enable netflow, simply specify IP of the server running FastNetMon and specify (configurable) port 2055

Why did we write this? Because we can't find any software for solving this problem in the open source world!

What is a "flow" in FastNetMon terms? It's one or multiple UDP, TCP, or ICMP connections with unique src IP, dst IP, src port, dst port, and protocol.

License: GPLv2

Project

- Official site
- Mailing list
- Release Notes
- If you want add an idea
- Chat: #fastnetmon at irc.freenode.net web client
- Detailed reference in Russian: link

Supported packet capture engines

- NetFlow v5, v9
- IPFIX
- sFlow v4 (since 1.1.3), v5
- Port mirror/SPAN capture with PF_RING (with ZC/DNA mode support need license), SnabbSwitch, NETMAP and PCAP

IPSERVERONE
Trusted . Reliable . Secured Hosting Provider

When a DDoS is detected, what is the mitigation plan?

Here are the typical **mitigation methods**:

Method	Null Route	Self-Mitigate	100% Cloud	Hybrid
Operation impact	IP got blocked	Can access as usual	Access as usual, but may be higher latency	Can access as usual
Cost to implement	FREE	Expensive	Manageable Cost	Expensive
Limitation	Not all IX support Null route	High cost and high technical skills	Latency issue	Skill set and cost.
Impact to the provider	Customer may be leaving	$$$	$	$$$$

Updates from MYIX:

MyIX route server is now **supporting blackhole community**

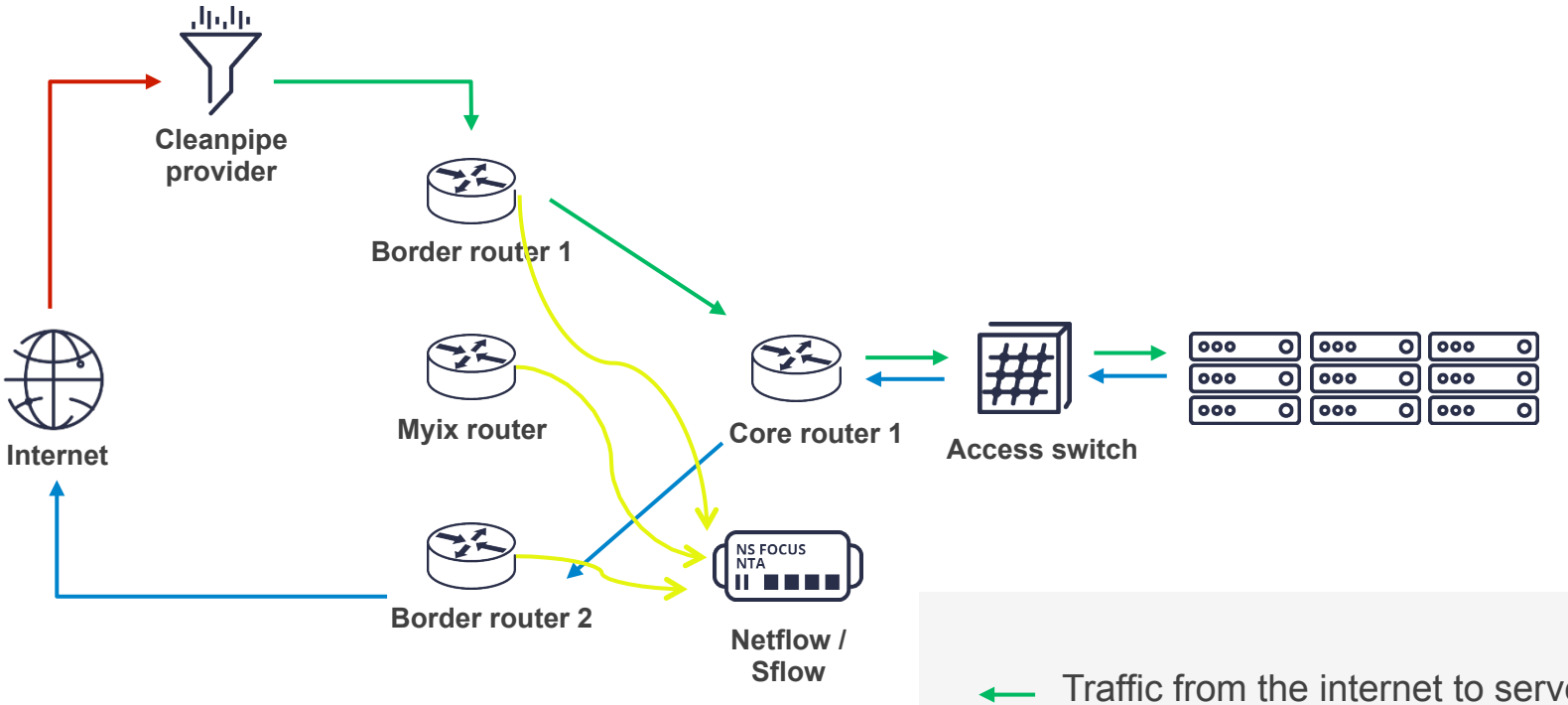
It may help on **reducing the DDoS attacks** from MyIX peering members that learned the route from MyIX route server

04.

How do we **Mitigate DDoS attacks** at IP ServerOne?

We send flows to our Network Traffic Analyzer

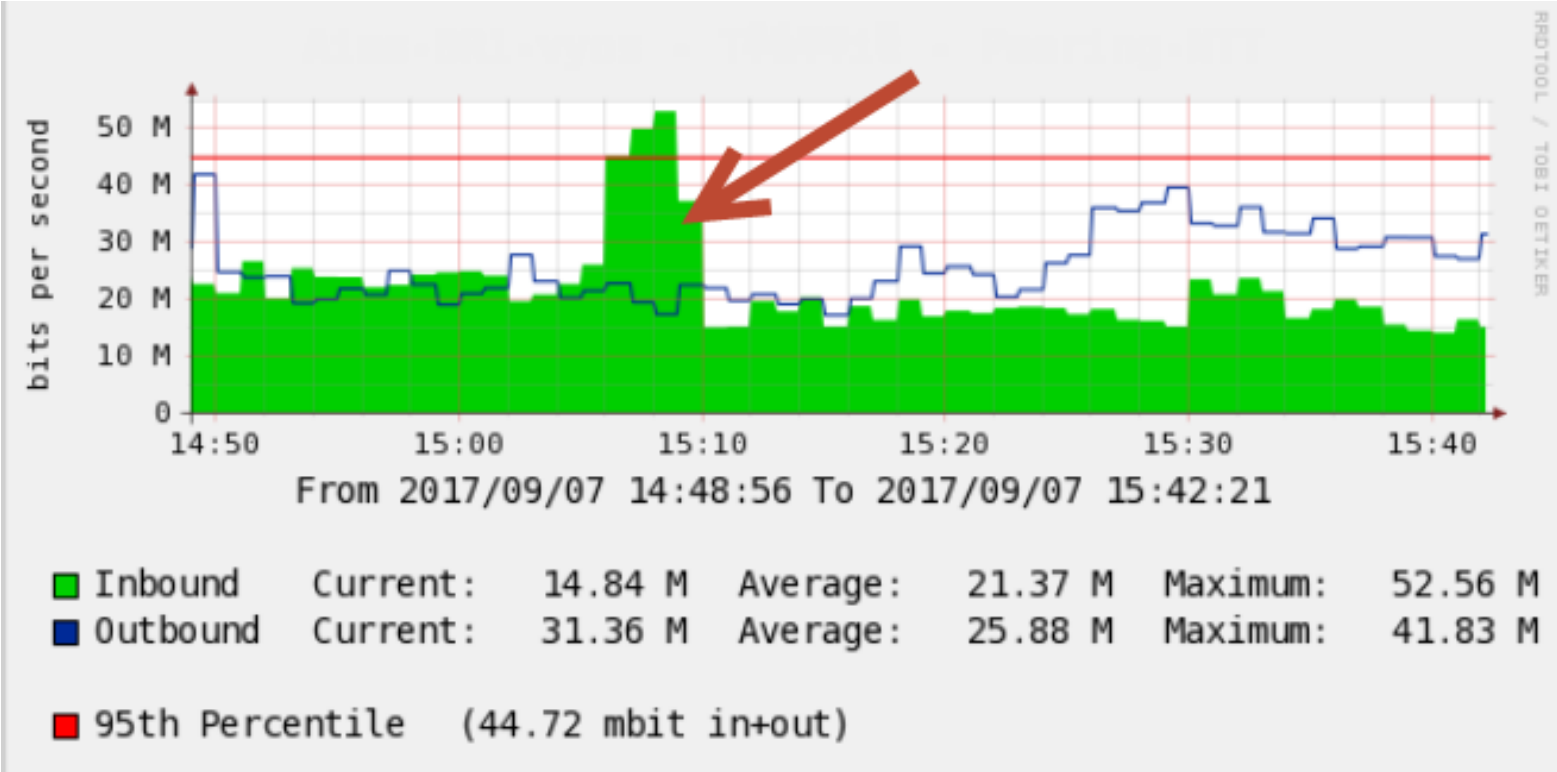
netflow will be sending from all our border routers



Traffic from the internet to server
Traffic from server to internet
Attack traffic

Time required for a DDoS Detection:

It may be taking less than **<u>90 seconds</u>**
to complete the **DDoS detection + mitigation**



DDoS Mitigation

At IP ServerOne, the Anti-DDoS is based on hybrid model
On-Premise device + Cloud based protection

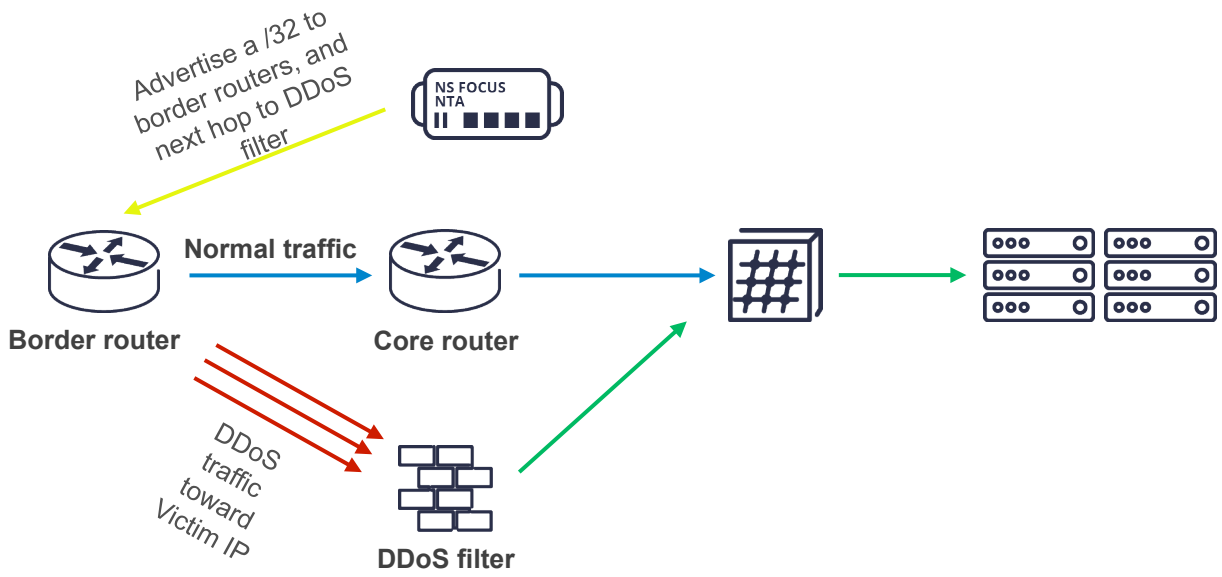
The reason why we are mitigating the attacks ourselves are:

Most of the cloud providers are **located overseas**

70% of our bandwidth is going through MyIX

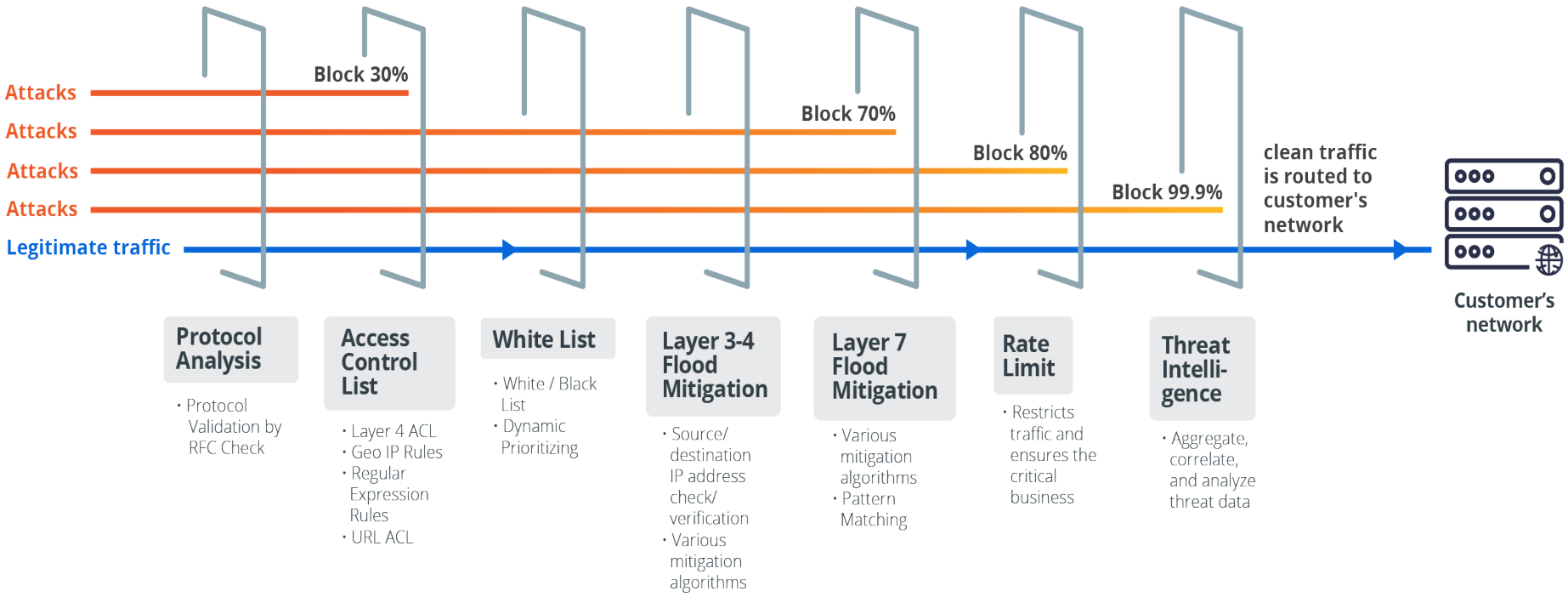
Cloud providers could have false positive sometime. Troubleshooting on this is very difficult; we are using **BGP communities to do traffic engineering**; so that those targetted customers will be coming through our own link rather than other cloud providers.

How do we deploy the mitigation device:



- When the victim's server IP is under attack
- The detector will **advertise a /32 over to all borders router**, so that all traffic towards the victim server will be next-hop to the filtering device for cleaning purpose
- **Traffic towards other servers is not affected**

What does the Anti-DDoS filter do?



05.

Where to **START?**

Where to start?

To combat against a DDoS, let's start with detection process first:

Commercial solution=
you can visit our booth

IPSERVERONE®
Trusted . Reliable . Secured Hosting Provider

Open-source solution=
fastnetmon
(we highly recommend trying this)

FASTNETMON

06.

ANY QUESTIONS?

Thanks

OUR INFRASTRUCTURE; YOUR GROWTH

E-mail: cllee@ip.my

Mobile: +6 012-331 9286

IP ServerOne Solutions Sdn. Bhd. (800140-T)
A-1-1 & A-1-2, Block A, Glomac Damansara,
Jalan Damansara, 60000 Kuala Lumpur,
Wilayah Persekutuan, Malaysia.

03 2026 1688
www.ipserverone.com

bsi. ISO/IEC 27001 Information Security Management

ISO Certificate No: IS 651738