

Detecting and mitigating attack DDoS in LV

Loi Tran Van
Long Van Cloud
loitv@longvan.net

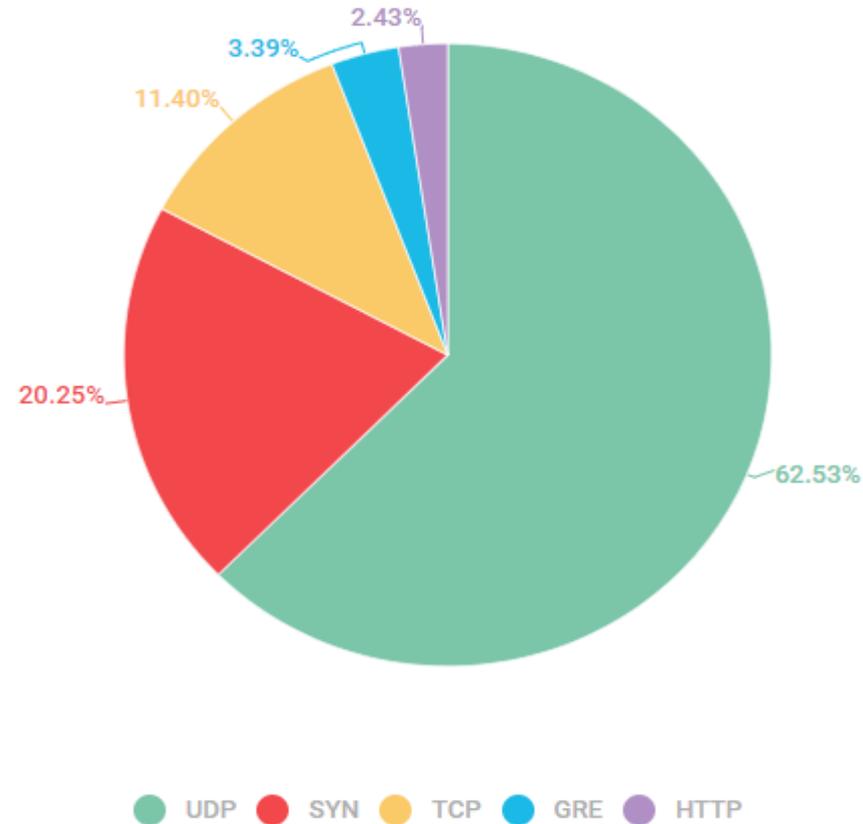
- Summary attack DDoS 2022
- Detecting and mitigating DDoS
- Monitor DDoS in Long Van
- QA

Summary attack DDoS 2022



➤ Quarter Summary in Q2 2022

- ✓ System recorded 78.588 DDos attacks
- ✓ 25% of the targets located in the US
- ✓ UDP flood accounted for 62.53 % off attacks
- ✓ Sys flooding 20.25%
- ✓ TCP flooding 11.4%
- ✓ Gre 3.39 %
- ✓ Http flooding 2.43 %

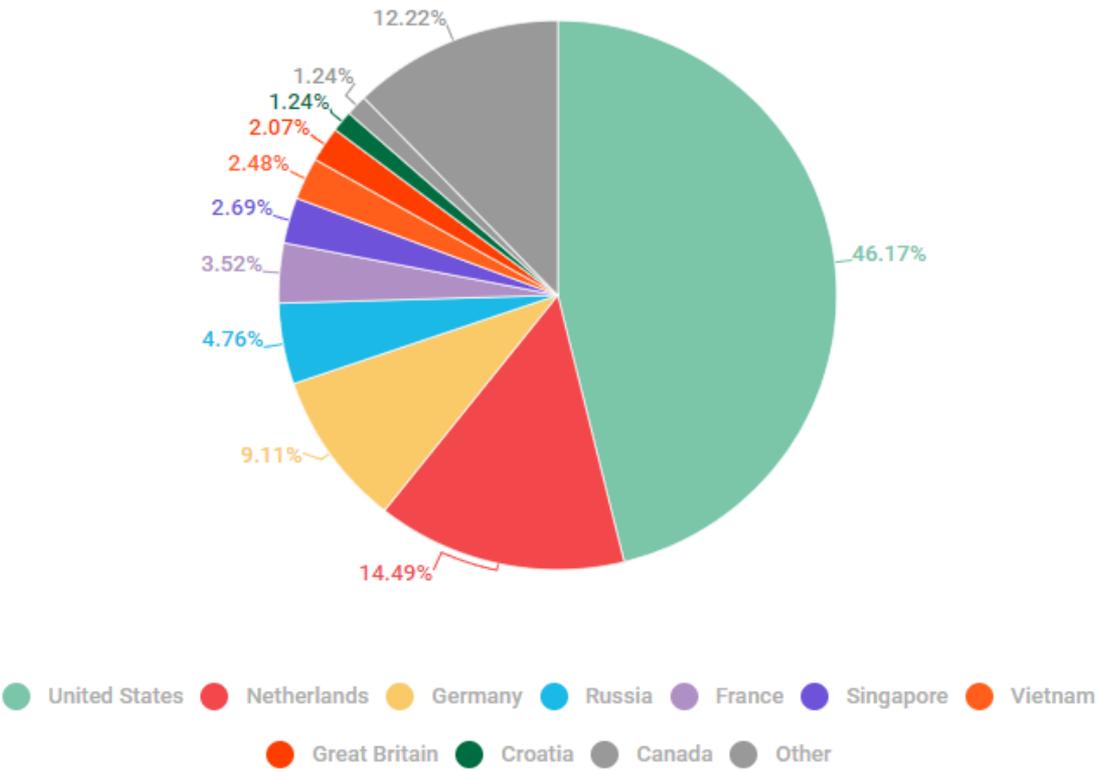


Summary attack DDoS 2022



➤ Geographic distribution of botnets

- ✓ USA 46.17 %
- ✓ Nertherlands 14.49 %
- ✓ Vietnam 2.07 %



Whats wrong with current DDoS equipment?

- ✓ Too Expensive
- ✓ Need dedicated qualified network engineers
- ✓ Not fully automated
- ✓ Complicated installation
- ✓ Unseless in case of channel onverflow

Whats wrong with ddos services?

- ✓ Increased lantency
- ✓ Still need tool for trigger traffic diversion/redirection
- ✓ No outgoing attack mitigation
- ✓ Sercurity reasons
- ✓ Service could be broken by attack to another client

Monitor DDoS in Long Van

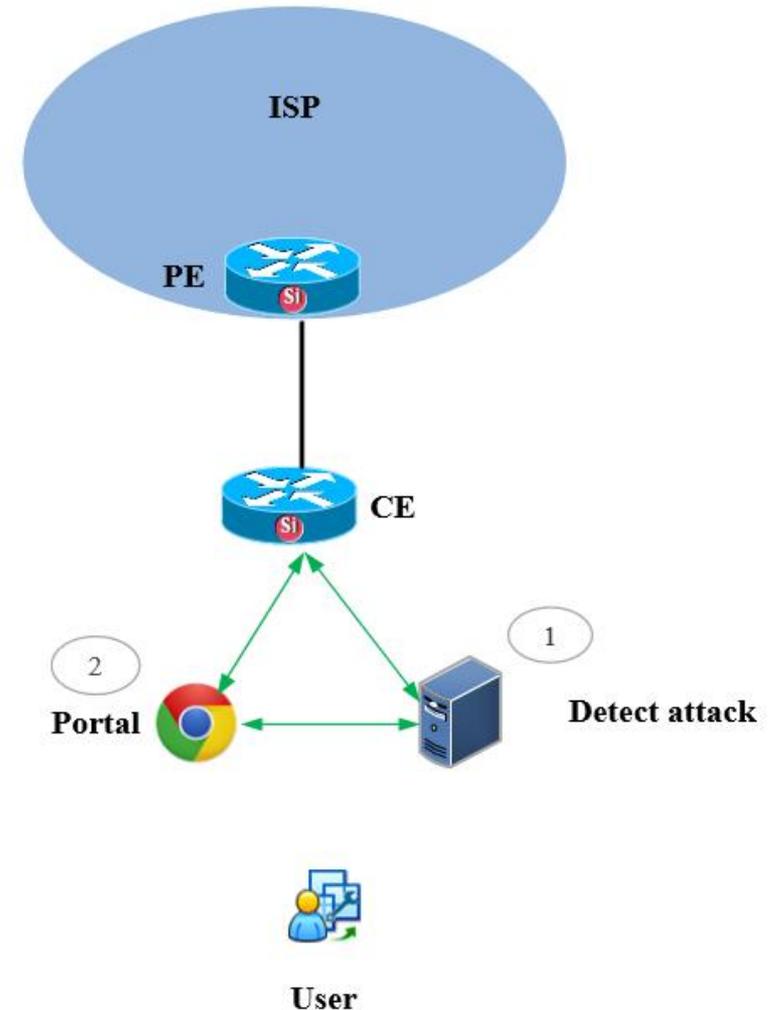
Components and Functional

1. Server monitor detect attack

- Detecting and mitigating attack
- Notification mail, Slack...

2. Web Portal

- Show detail ip attack, type, history attack
- Get status ip on Router CE
- Allow user manual block, unblock IP attack on Router CE
- Send alarm for customer



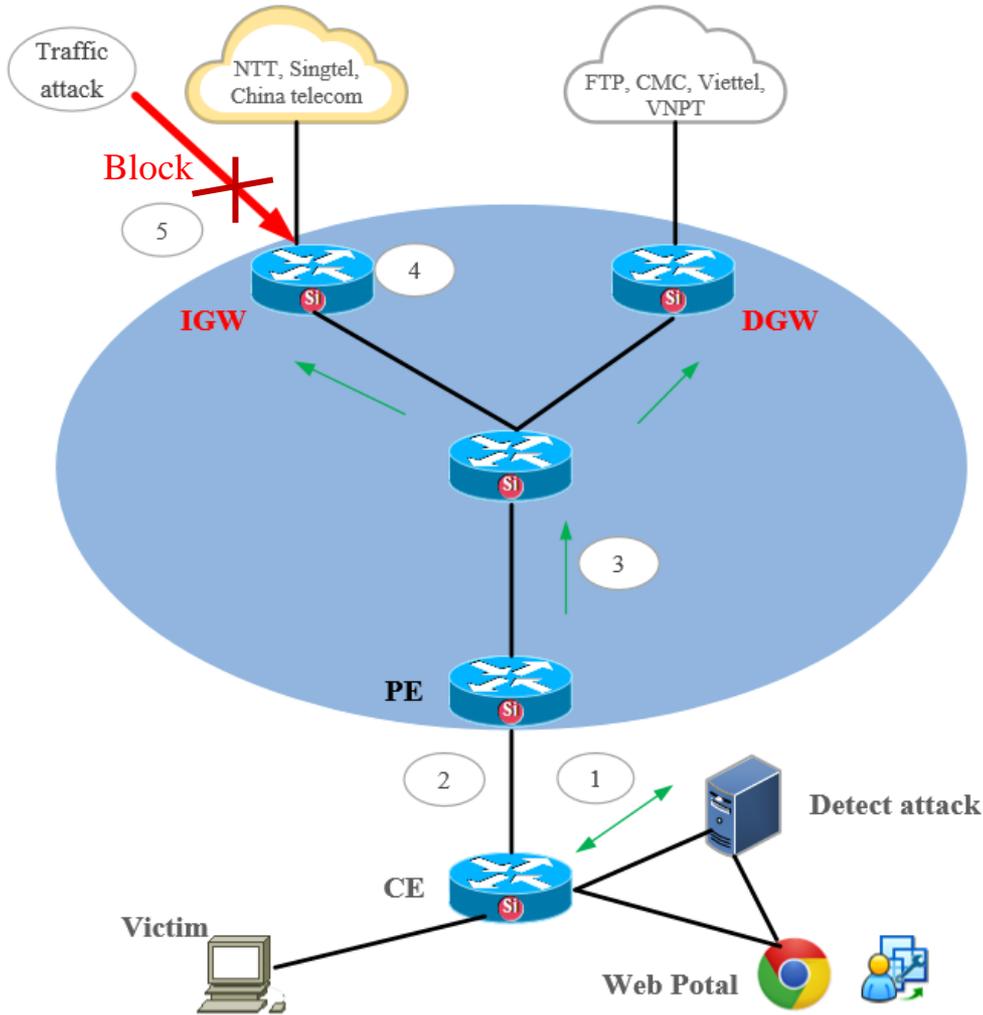
Monitor DDoS in Long Van



Meet the Requires monitoring system

- ✓ Fast attack detection, Fast mitigation and isolation
- ✓ Fully Automatic
- ✓ Unlimited scalability (10-20Gbs-1-2 Tbps)
- ✓ Reduce Cost
- ✓ Notification attack (Graph web, Mail, Slack, webhook..)
- ✓ Easy install, easy integration with scrubbing centres
- ✓ Support any more platform

How does it work ?



1. Udp_flood attack detected, blackhole host route setup in ExaBGP
2. BGP advertise route tager ip addresss/32 community 3128:911
3. Blackhole host route distributed to all sysnet routers
4. Blackhole host route distributed with appropriate community to peers accepting blackhole route
5. Acttack block at egde of provider networks accepting blackhole route

Note

IGW : International Gateway

DGW : Domestic Gateway

Notification Alarm



Notification attack on Graph



Portal DDoS Long Van



Show status ip attack on Portal

Long Vân System

Search

- Dashboard
- Check Event IP
- Manual Block/Unblock
- DC Config
- AS Config
- Routers Config

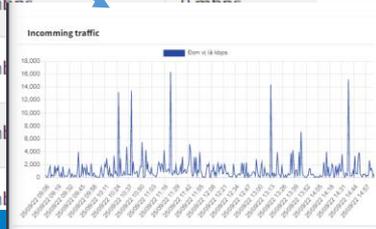
84 Warning Blocked
From 25/09/2022 08:55 to 25/09/2022 14:55
More Blocked

85 Warning Unblocked
From 25/09/2022 08:55 to 25/09/2022 14:55
More UnBlocked

Show entries

STT	Time latest	IP address	Type	Incoming traffic
1	25/09/22 14:52	103.48.194.137	Blocked Attack	1 mbps
2	25/09/22 14:51	103.48.194.137	Unblocked Attack	0 mbps
3	25/09/22 14:46	45.119.215.151	Blocked Attack	1 mbps
4	25/09/22 14:42	45.119.215.151	Unblocked Attack	0 mbps
5	25/09/22 14:42	103.48.194.173	Blocked Attack	0 mbps
6	25/09/22 14:41	103.48.194.173	Unblocked Attack	0 mbps
7	25/09/22 14:40	103.48.193.51	Unblocked Attack	1 mbps
8	25/09/22 14:40	103.48.194.152	Blocked Attack	0 mbps
9	25/09/22 14:39	103.48.194.152	Unblocked Attack	0 mbps
10	25/09/22 14:32	103.48.194.141	Blocked Attack	4 mbps

IP Address	45.119.215.151
Incoming Traffic	1 mbps
Outgoing Traffic	10 mbps
Incoming PPS	109583
Outgoing PPS	59224
Attack uuid	eccd48f7-3148-4da5-be88-3186413514c0
Attack severity	middle
Attack type	unknown
Initial attack power	109583
Peak attack power	109583
Total incoming flows	IPv4
Total outgoing flows	0
Incoming ip fragmented traffic	0 mbps



Search infor customer from ip attack, check send mail, or call

Long Vân System

IP Address: **103.48.194.137** Service code: **19402186** Customer: **SC-POOL23** Email: **hinhmd@gmail.com** Status: **Active**

IP  103.48.194.137 From 25/09/2022 08:58  To 25/09/2022 14:58  All Type < 

11 Warning Blocked From 25/09/2022 08:58 to 25/09/2022 14:58 

11 Warning Unblocked From 25/09/2022 08:58 to 25/09/2022 14:58 

Show entries Search:

STT ↑↓	Time ↑↓	IP Check ↑↓	Type ↑↓	Incoming traffic ↑↓	Outgoing traffic ↑↓	Incoming pps ↑↓	Outgoing pps ↑↓	Email ↑
1	25/09/22 14:52	103.48.194.137	Blocked Attack	1 mbps	0 mbps	144013	24566	
2	25/09/22 14:51	103.48.194.137	Unblocked Attack	0 mbps	0 mbps	103392	28459	
3	25/09/22 14:19	103.48.194.137	Blocked Attack	0 mbps	0 mbps	103392	28459	
4	25/09/22 14:17	103.48.194.137	Unblocked Attack	0 mbps	0 mbps	110915	188	
5	25/09/22 13:46	103.48.194.137	Blocked Attack	0 mbps	0 mbps	110915	188	
6	25/09/22 13:44	103.48.194.137	Unblocked Attack	0 mbps	0 mbps	102002	3921	
7	25/09/22 13:13	103.48.194.137	Blocked Attack	0 mbps	0 mbps	102002	3921	
8	25/09/22 13:11	103.48.194.137	Unblocked Attack	0 mbps	0 mbps	109494	2846	

User manual block or unlock IP attack direct to router

Long Vân System

Search

- Dashboard
- Check Event IP
- Manual Block/Unblock**
- DC Config
- AS Config
- Routers Config

IP Block [Block Now](#)

Show 10 entries Search:

STT	IP Blocked	DC	AS	Routers	Action
1	103.125.168.34	United States	123 test	DC4-HCM	Unblock
2	103.27.223.13	United States	123 test	DC4-HCM	Unblock
3	103.125.168.33	United States	123 test	DC4-HCM	Unblock
4	103.125.168.32	United States	123 test	DC4-HCM	Unblock
5	103.125.168.125	United States	123 test	DC4-HCM	Unblock
6	103.125.168.122	United States	123 test	DC4-HCM	Unblock
7	103.34.45.15	United States	123 test	DC4-HCM	Unblock
8	103.125.168.12	United States	123 test	DC4-HCM	Unblock
9	103.125.168.67	United States	123 test	DC4-HCM	Unblock
10	103.48.192.43	Canada	345	DC7-HCM	Unblock

Tools

- BIRD (for BGP) - <http://bird.network.cz/>
- FastNetMon -
[https://github.com/FastVPSEestiOu/
fastnetmon](https://github.com/FastVPSEestiOu/fastnetmon)
&&
<http://fastvpseestiou.github.io/fastnetmon/>

Q&A

