LONG VAN
System Solution

Detecting and mitigating attack DDoS in LV

Loi Tran Van
Long Van Cloud
loitv@longvan.net

Agenda

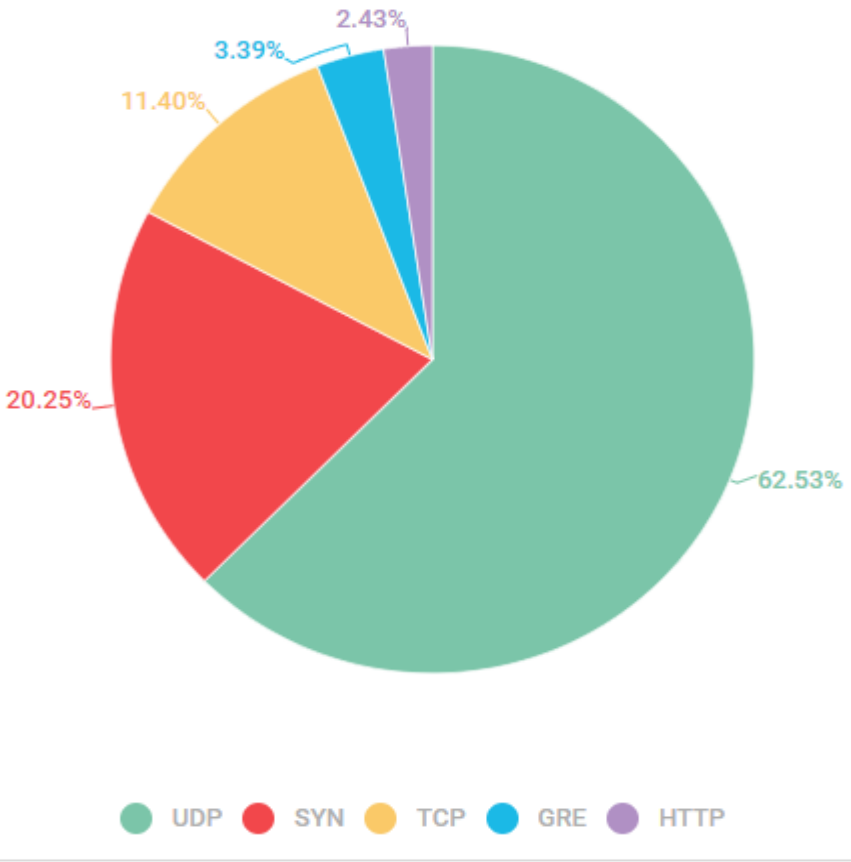
- Summary attack DDoS 2022
- Detecting and mitigating DDoS
- Monitor DDoS in Long Van
- QA

Summary attack DDoS 2022

LONG VAN System Solution

➢ 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 %

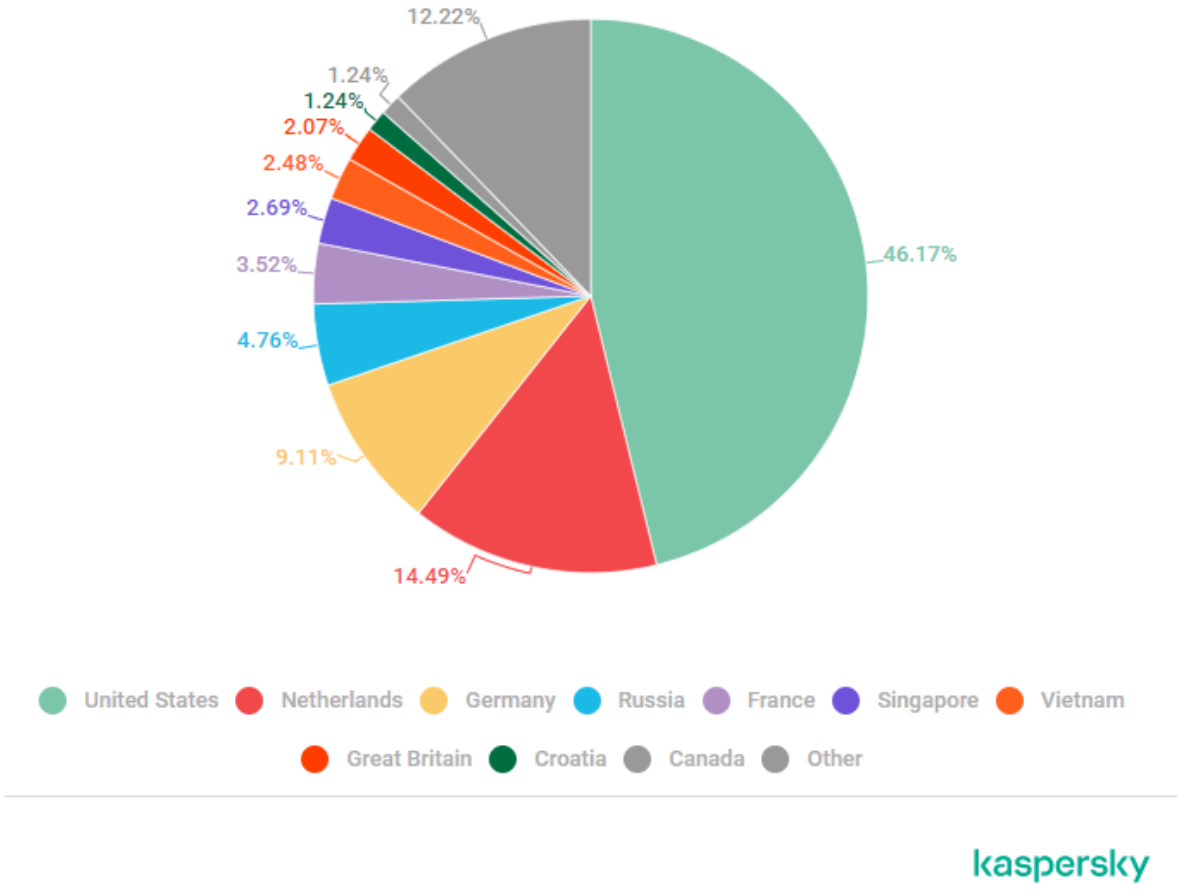


Summary attack DDoS 2022

LONG VAN System Solution

➢ Geographic distribution of botnets

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



LONG VAN
System Solution

Whats wrong with current DDoS equipment?

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

LONG VAN
System Solution

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

LONG VAN System Solution

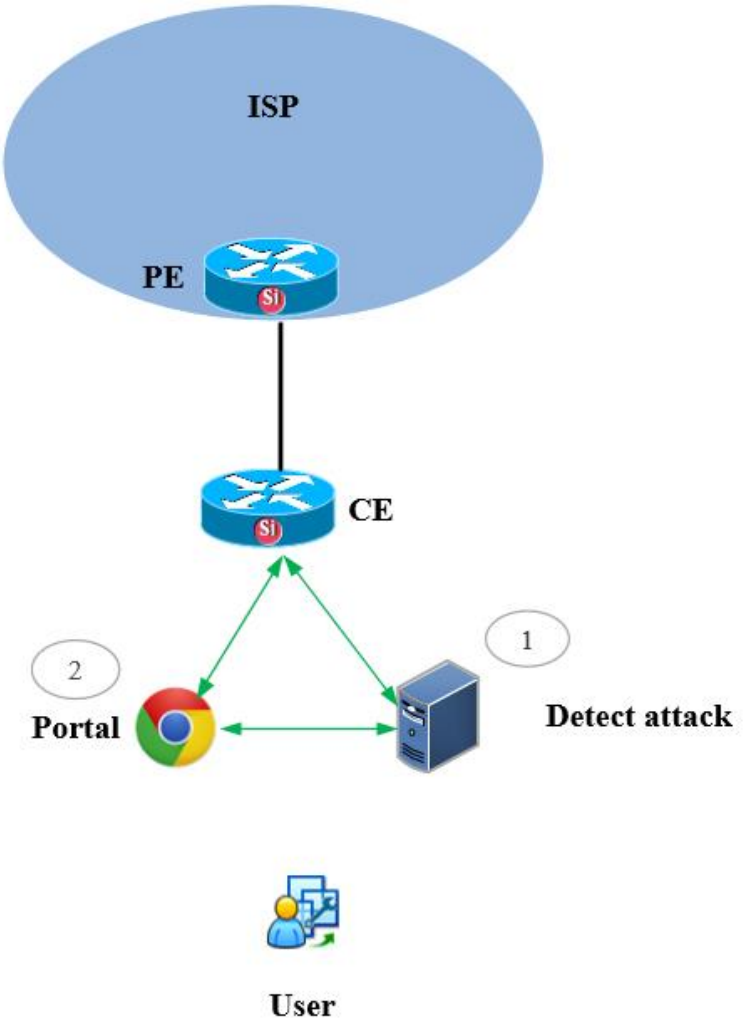
Components and Functional

1. **Server monitor detect attack**

- Detecting and mitigating attack
- Notificaction 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



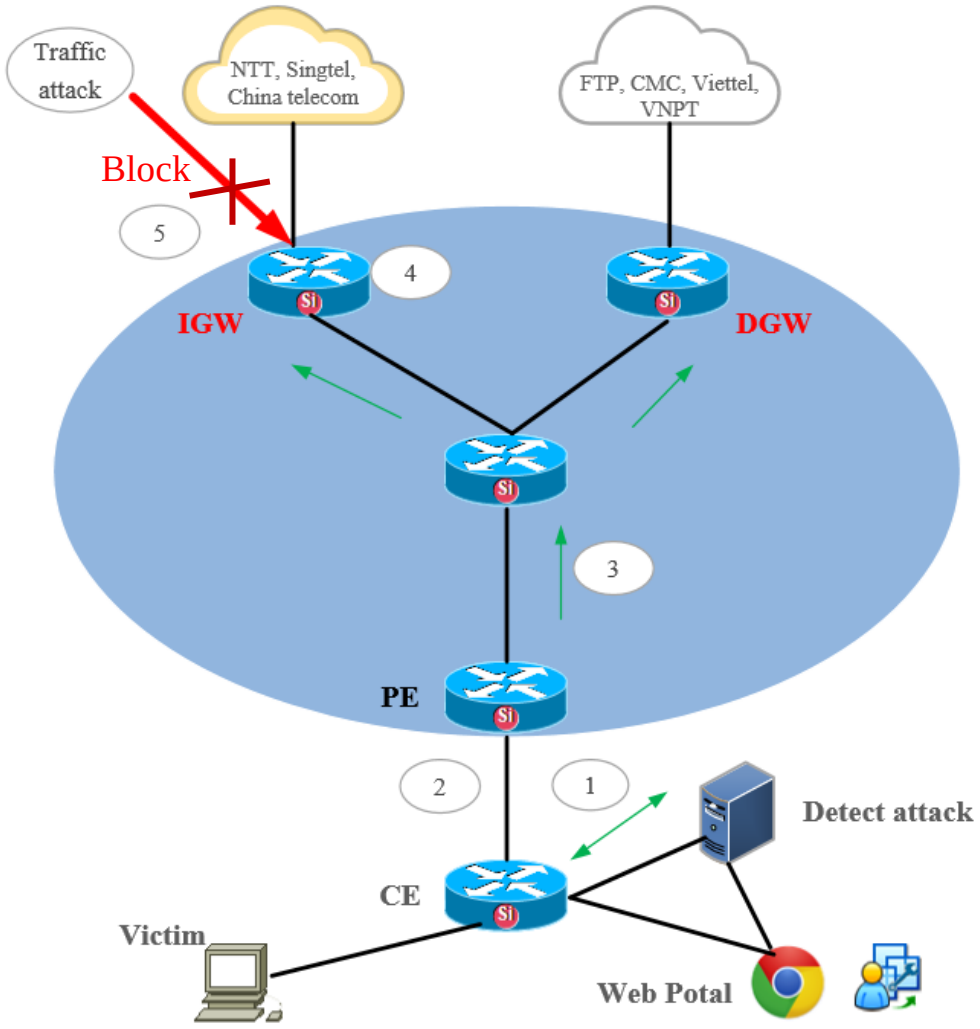
Monitor DDoS in Long Van

LONG VAN
System Solution

Meet the Requires monitoring system

- ✓ Fast attack detection, Fast mitigation and isolation
- ✓ Fully Automatic
- ✓ Unlimited scaclability (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

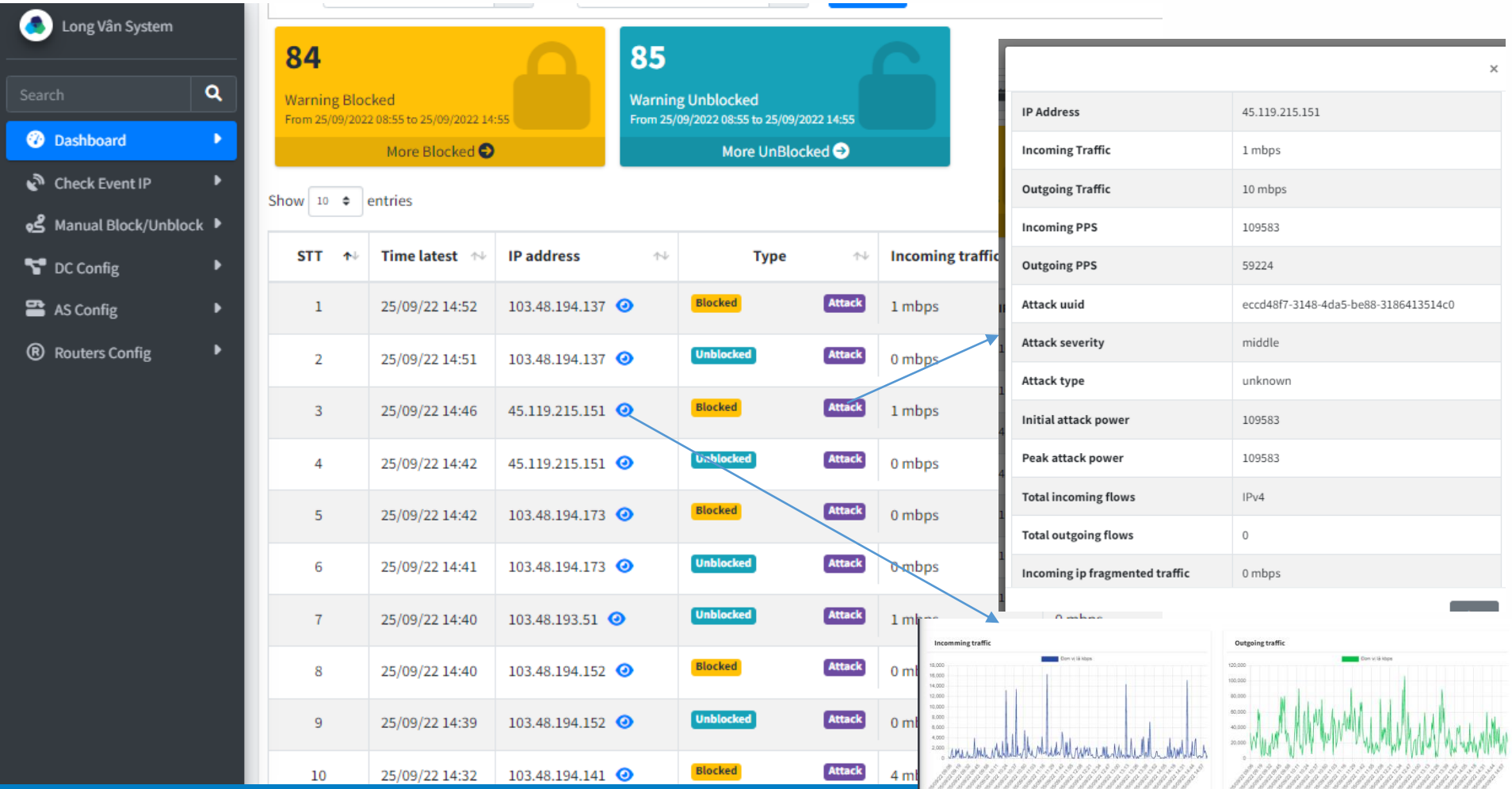
LONG VAN
System Solution

Notification attack on Graph

Portal DDoS Long Van

LONG VAN System Solution

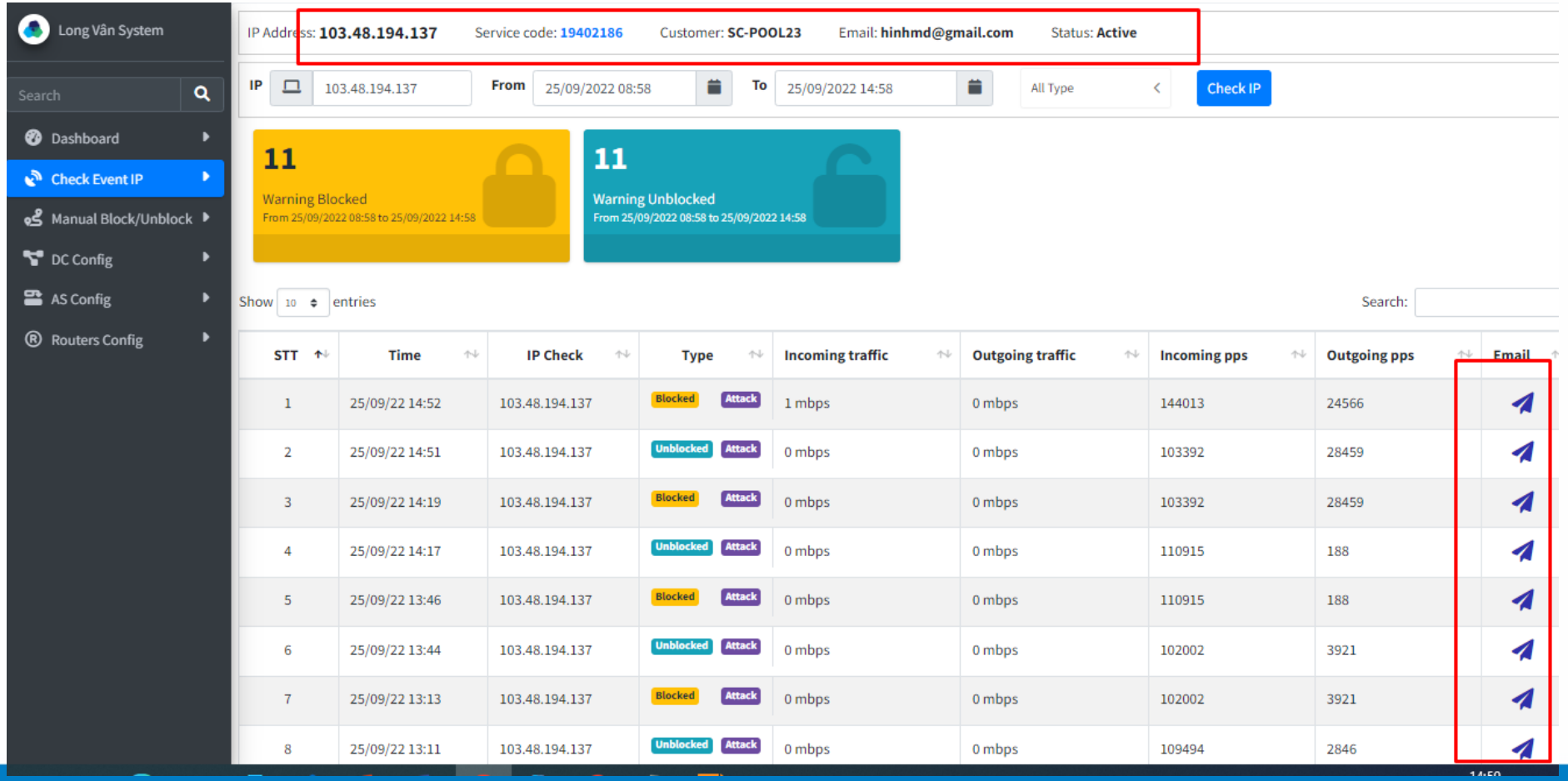
Show status ip attack on Portal



Portal DDoS Long Van

LONG VAN System Solution

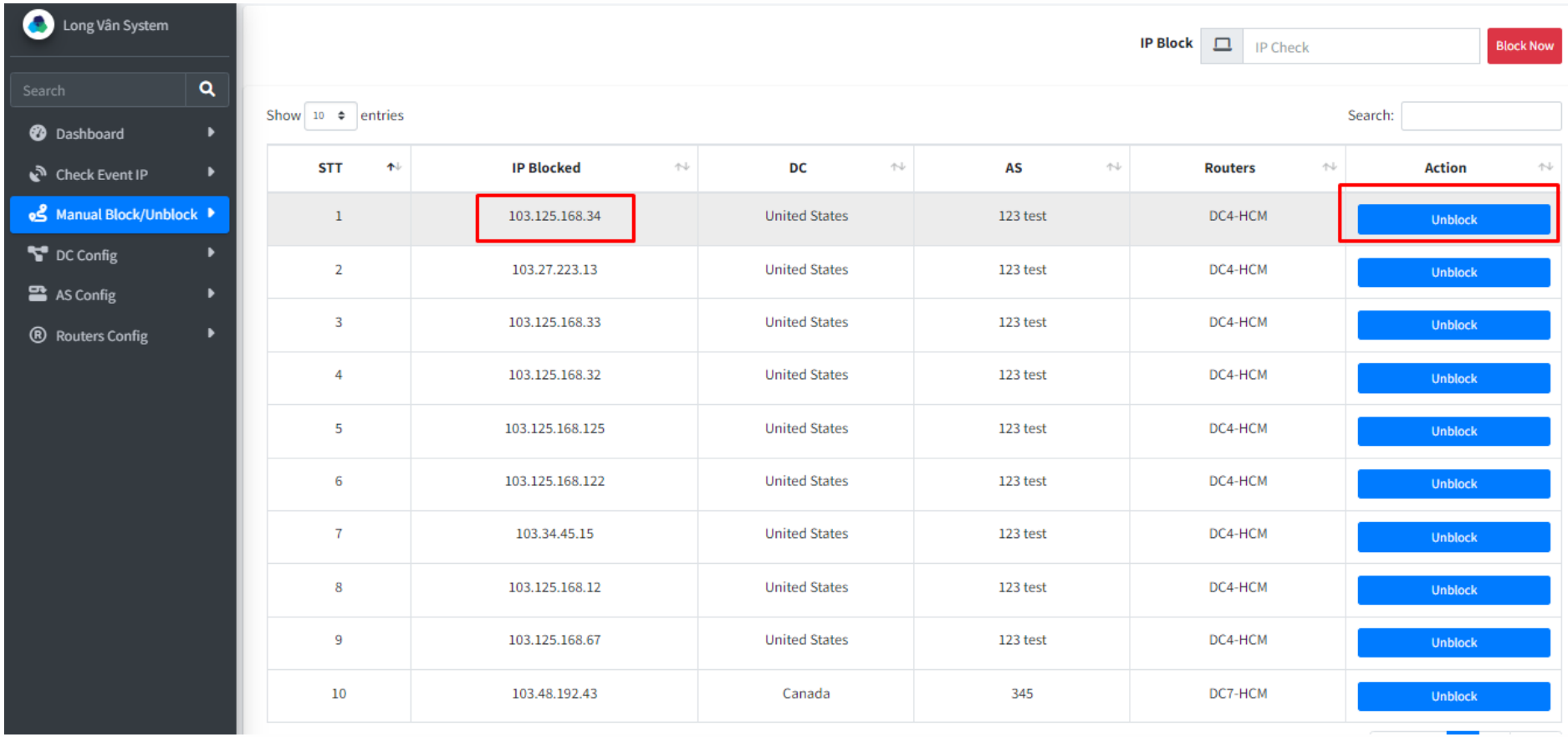
Search infor custormer from ip attack, check send mail, or call



Portal DDoS Long Van

LONG VAN System Solution

User manual block or unlock IP attack driect to router



Document refer

LONG VAN
System Solution

Tools

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

LONG VAN
System Solution

Q&A