DDoS attacks from IXPs. Customer perspective

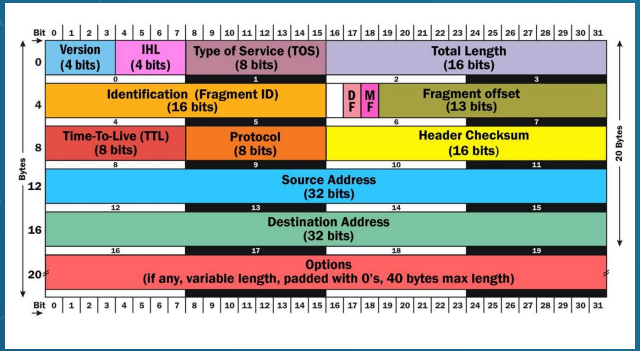
Hello

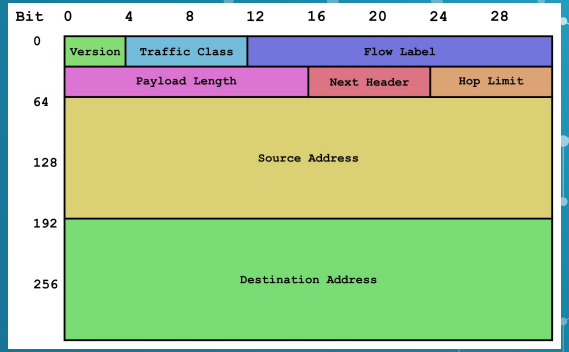
I'm Pavel Odintsov, the author of open source DDoS detection tool, FastNetMon Community: https://github.com/pavel-odintsov/fastnetmon

Ways to contact me:

- linkedin.com/in/podintsov
- github.com/pavel-odintsov
- twitter.com/odintsov_pavel
- IRC, Libera Chat, pavel_odintsov
- pavel@fastnetmon.com

What kind of DDoS? IPv4, IPv6: L3, L4





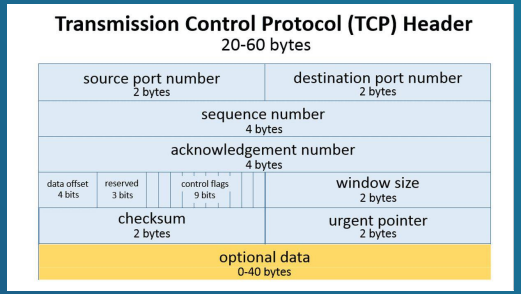
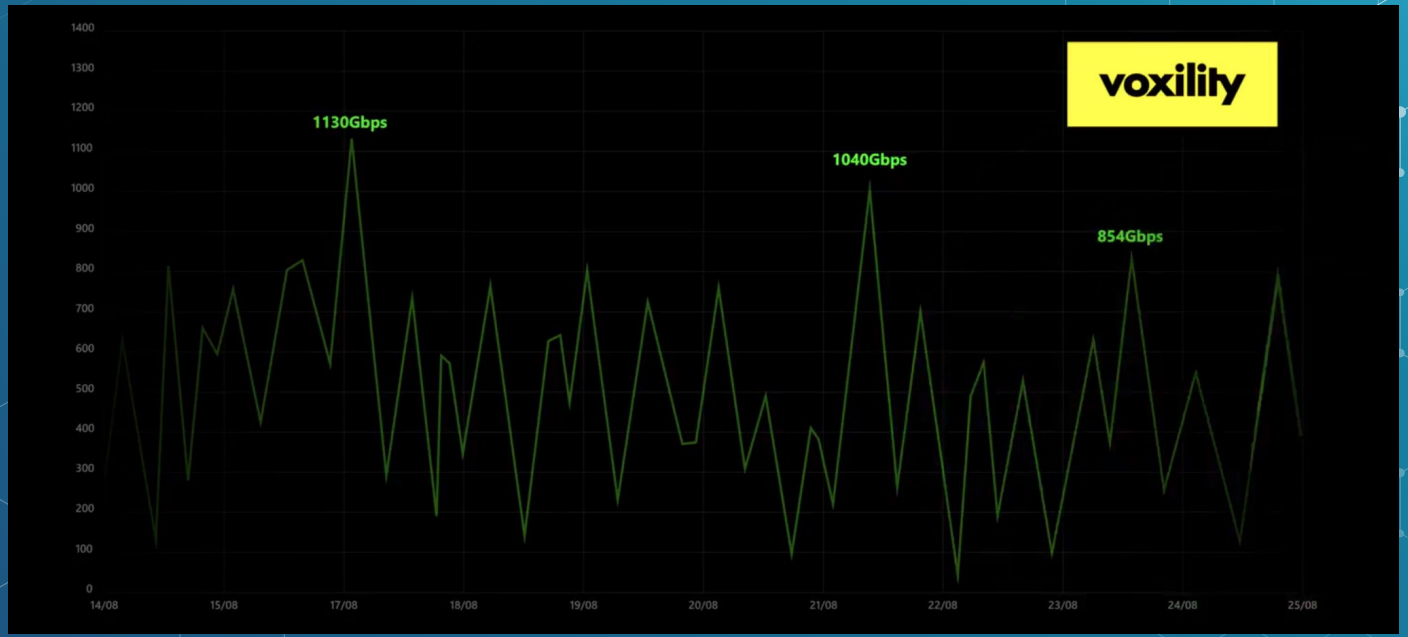


Image from https://thirdinternet.com/ip-packet-syntax/

What kind of DDoS? Attack names

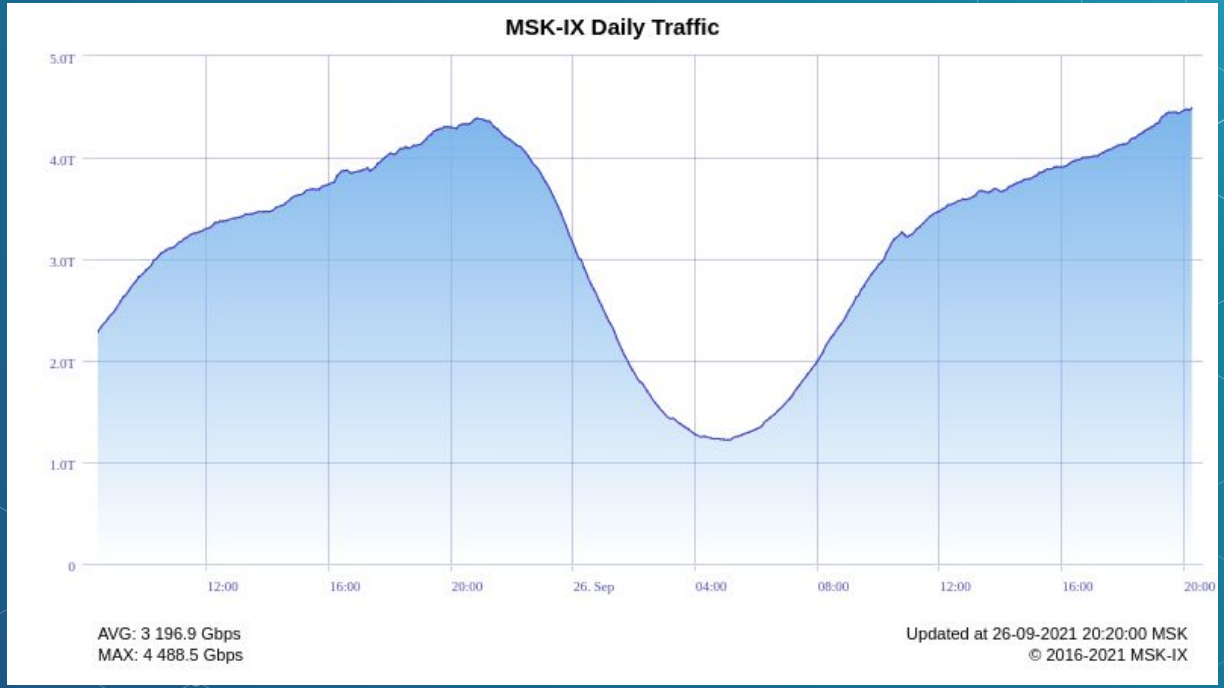
- TCP flag flood (i.e. SYN, ACK flood)
- UDP flood
- GRE flood
- UDP amplification (DNS, NTP, SSDP, SNMP)
- Fragmentation attack
- Spoofed source attacks

What is the DDoS weather this summer?



Data provided by Voxility.com

Can IXPs handle such large DDoS?



Data provided by MSK-IX

What about spare capacity at IXP?

Peering VLAN

Peering with MSK-IX participants directly or via Route Server

Private VLANs

Virtual circuits and private networks between MSK-IX PoPs

8 Tbps

Ethernet interconnection platform

Network redundancy built upon the **'Dual Core' topology**

Monitoring, security audits and customer support 24x7

- 1G, 10G, 100G Interfaces
- Etherchannel (LACP). Aggregating multiple physical interfaces in a single logical port.
- Trunk ports. Setting up multiple VLANs on one physical interface.
- Q-in-Q tunneling. Transparent forwarding of participants' own VLANs.

Data provided by MSK-IX

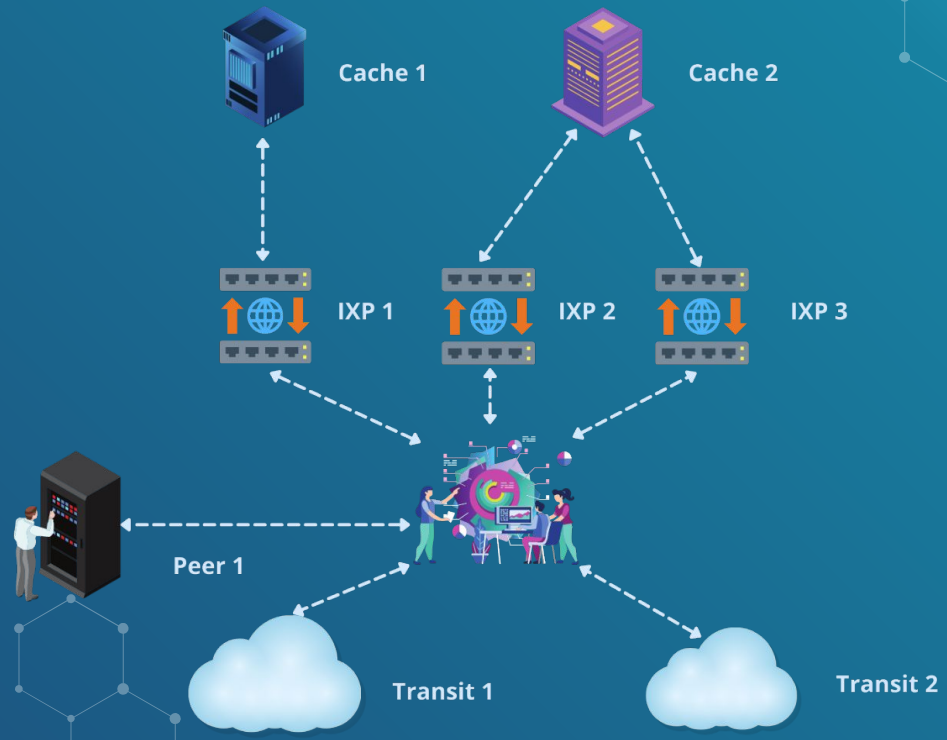
What about current capacity of MSK-IX?

- 152 Terabits
- 400G testing and waiting for customers
- Current 400G platform: 8*400G

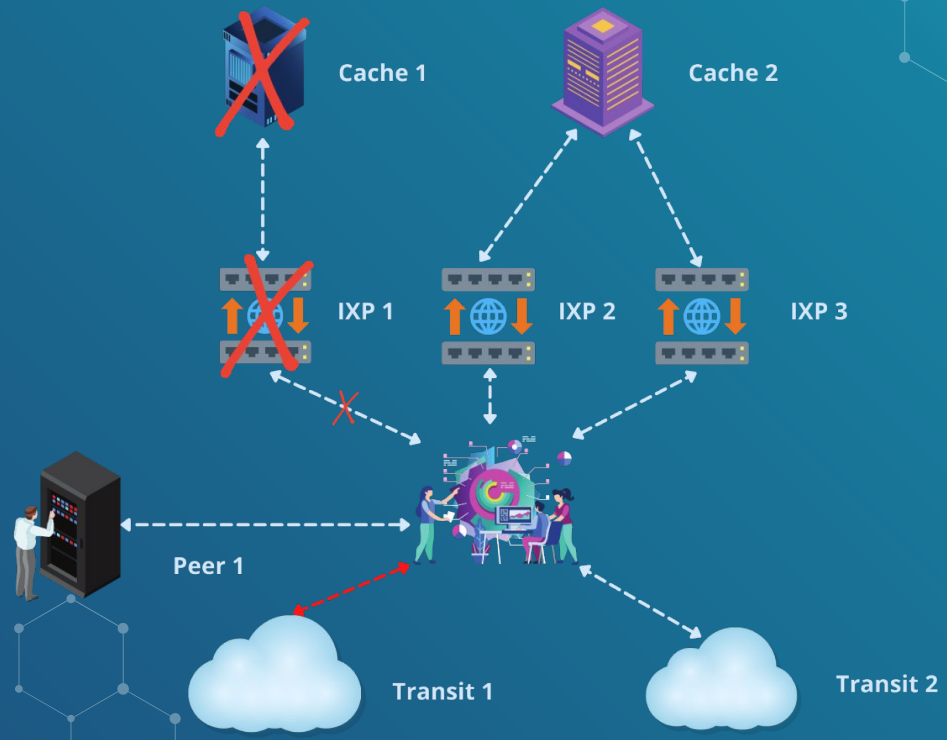
Data provided by MSK-IX

What is the problem?

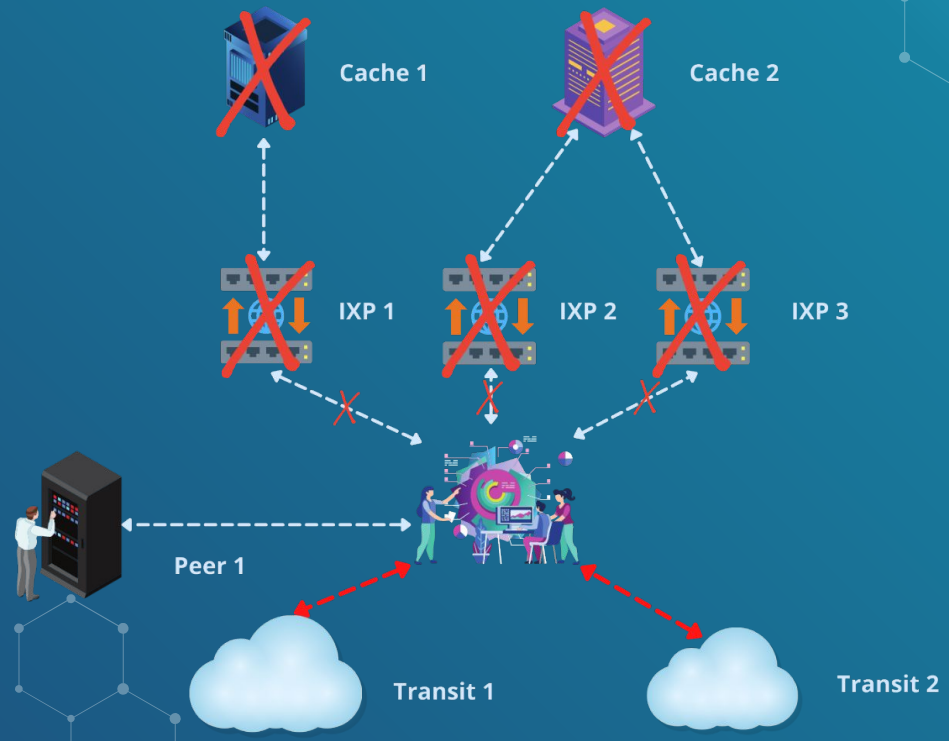
What is the common ISP setup?



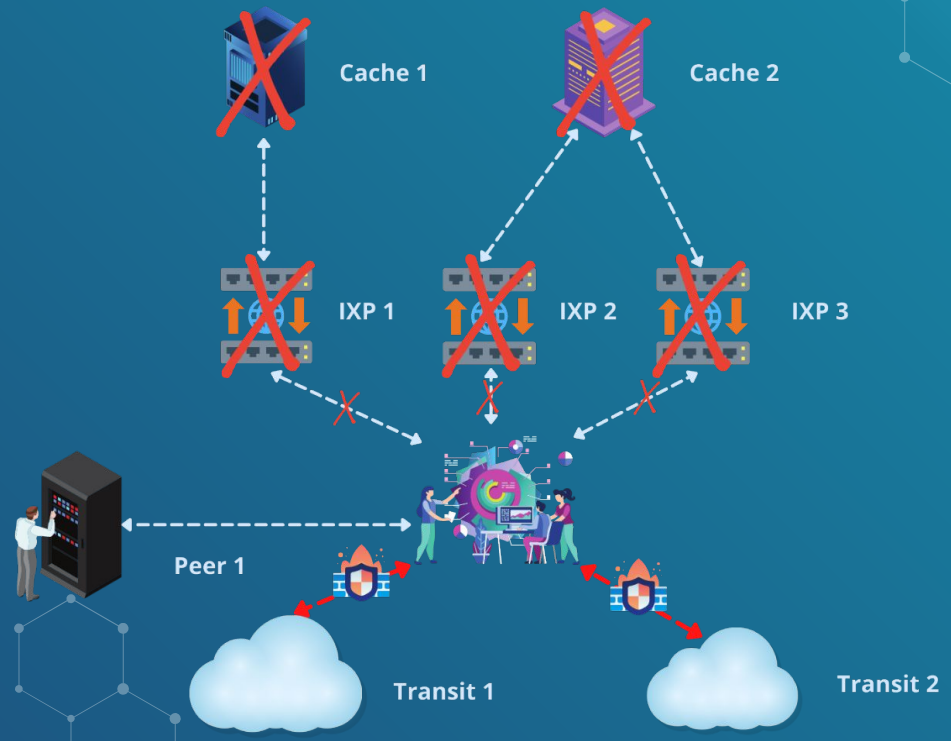
What can be done to stop an attack from IXP?



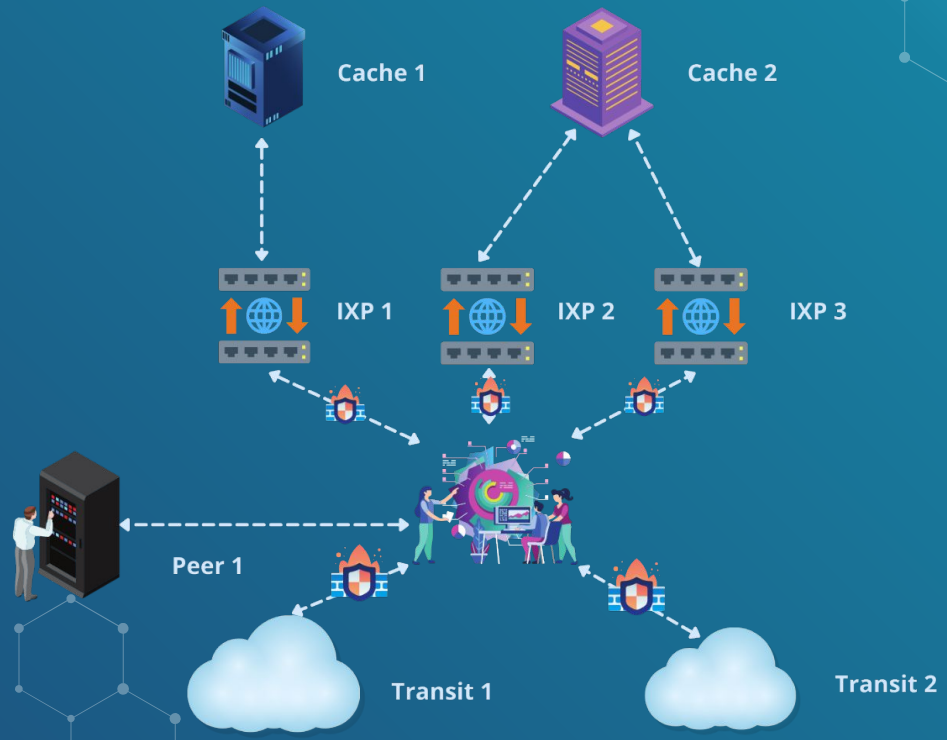
What can be done to stop an attack from IXPs?



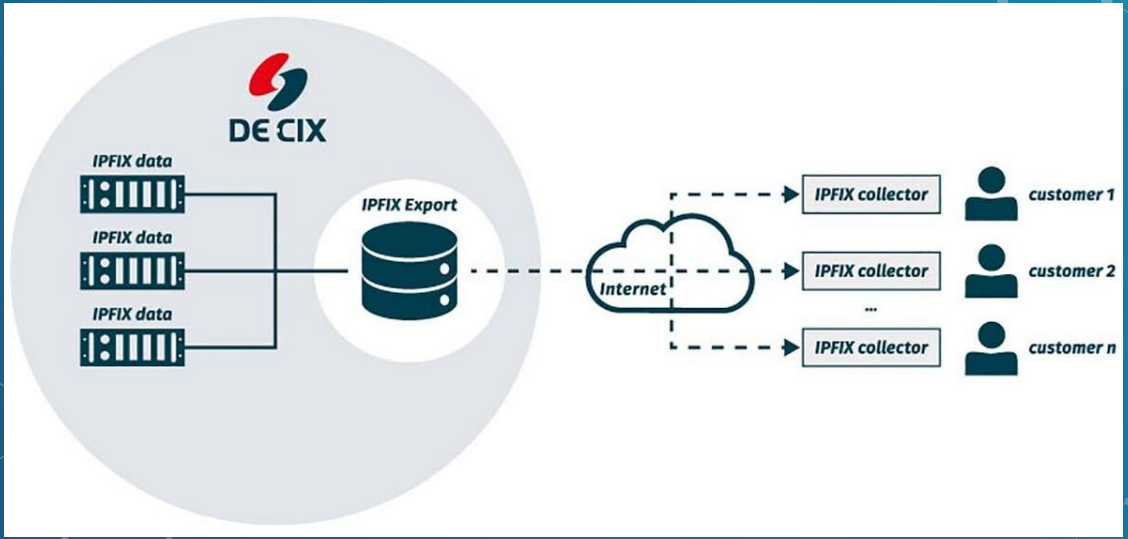
What is the most secure configuration now?



What is the best configuration?



Traffic telemetry: sharing is caring



FastNetMon Community: features

- Supports all types of volumetric attacks
- Does not require changes in your network
- Works on any Linux platform
- Complete automation
- Lightning fast detection: 5-30 seconds detection
- Great scalability (1T+ on single server)
- Software only solution
- BGP integration
- Support almost all possible traffic capture engines (sFlow, Netflow, IPFIX)

FastNetMon: attack actions

- BGP announces (ExaBGP, GoBGP)
- Slack notification
- Script call

FastNetMon Community Installation

- wget https://install.fastnetmon.com/installer -Oinstaller
- sudo chmod +x installer
- sudo ./installer -install_community_edition

FastNetMon: detection logic

Detection type:

- Threshold based (based on host's average traffic)

Threshold types:

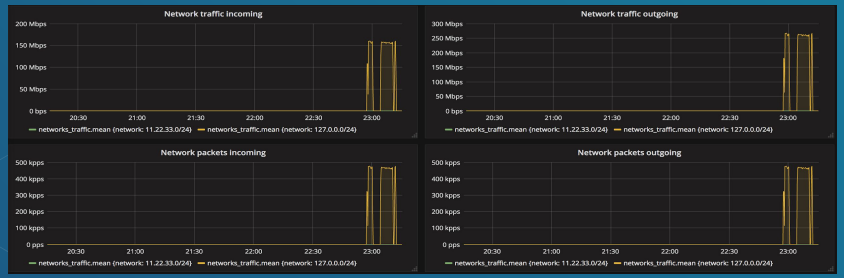
- Using total traffic
- Using total pps rate
- Per protocol

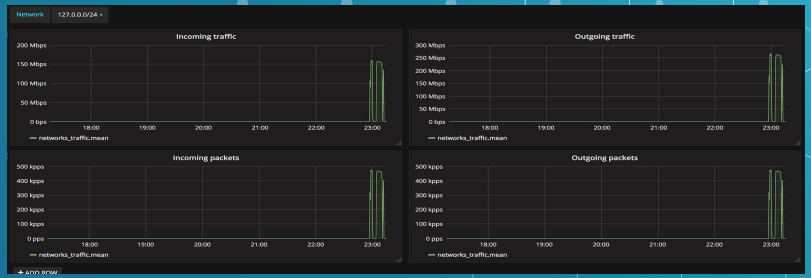
FastNetMon: attack reports

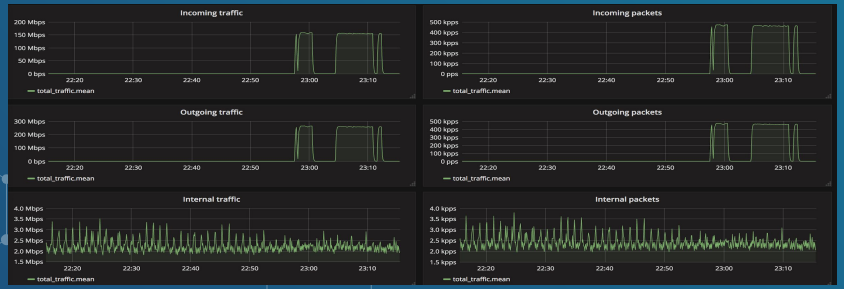
IP: 10.10.10.221Attack type: syn_flood
Initial attack power: 546475 packets per second
Peak attack power: 546475 packets per second
Attack direction: incoming
Attack protocol: tcp
Total incoming traffic: 245 mbps
Total outgoing traffic: 0 mbps
Total incoming pps: 99059 packets per second
Total outgoing pps: 0 packets per second
Total incoming flows: 98926 flows per second
Total outgoing flows: 0 flows per second
Average incoming traffic: 45 mbps
Average outgoing traffic: 0 mbps
Average incoming pps: 99059 packets per second
Average outgoing pps: 0 packets per second
Average incoming flows: 98926 flows per second
Average outgoing flows: 0 flows per second

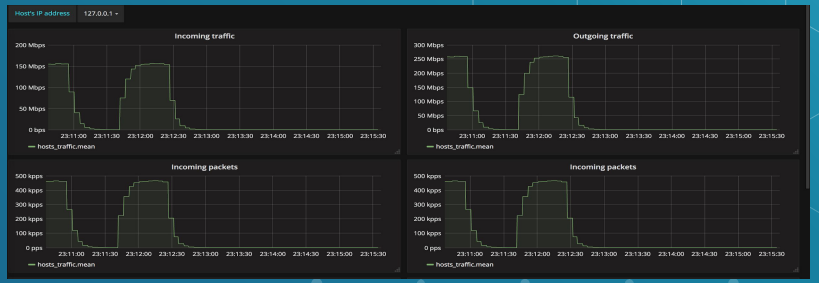
IP: 10.10.10.221Attack type: syn_flood
Initial attack power: 546475 packets per second
Peak attack power: 546475 packets per second
Attack direction: incoming
Attack protocol: tcp
Total incoming traffic: 245 mbps
Total outgoing traffic: 0 mbps
Total incoming pps: 99059 packets per second
Total outgoing pps: 0 packets per second
Total incoming flows: 98926 flows per second
Total outgoing flows: 0 flows per second
Average incoming traffic: 45 mbps
Average outgoing traffic: 0 mbps
Average incoming pps: 99059 packets per second
Average outgoing pps: 0 packets per second
Average incoming flows: 98926 flows per second
Average outgoing flows: 0 flows per second

FastNetMon: traffic reports in Grafana









FastNetMon: our community

- Site: https://fastnetmon.com/guides/
- GitHub: https://github.com/pavel-odintsov/fastnetmon
- IRC: #fastnetmon at Libra Chat
- Telegram: https://t.me/fastnetmon
- Slack: http://bit.ly/2o5Idx8
- LinkedIN: https://www.linkedin.com/company/fastnetmon/
- Facebook: https://www.facebook.com/fastnetmon/
- WhatsApp: https://chat.whatsapp.com/JjwF855pwZvIIasTUsZ7EO

THANKS!

ANY QUESTIONS?

You can find me at:

- @odintsov_pavel
- pavel@fastnetmon.com
- linkedin.com/in/podintsov