DDoS Detection and Traffic visibility for IXPs

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? L3. IPv4

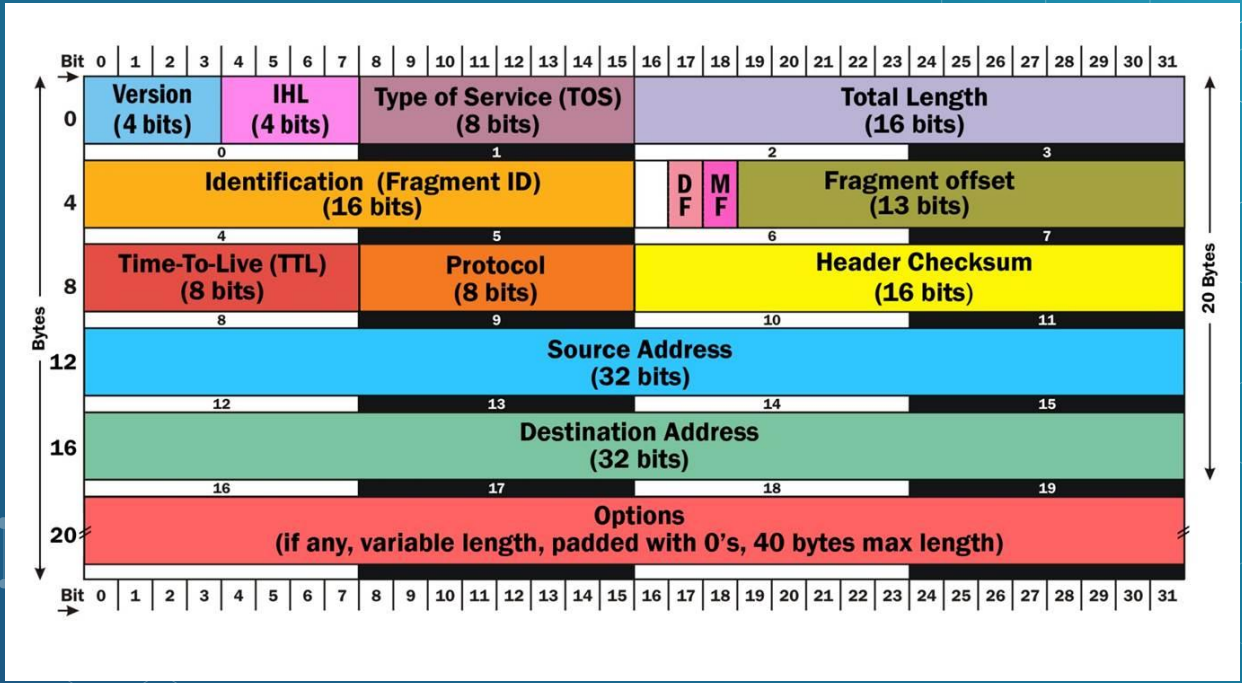


Image from https://thirdinternet.com/ip-packet-syntax/

What kind of DDoS? L3. IPv6

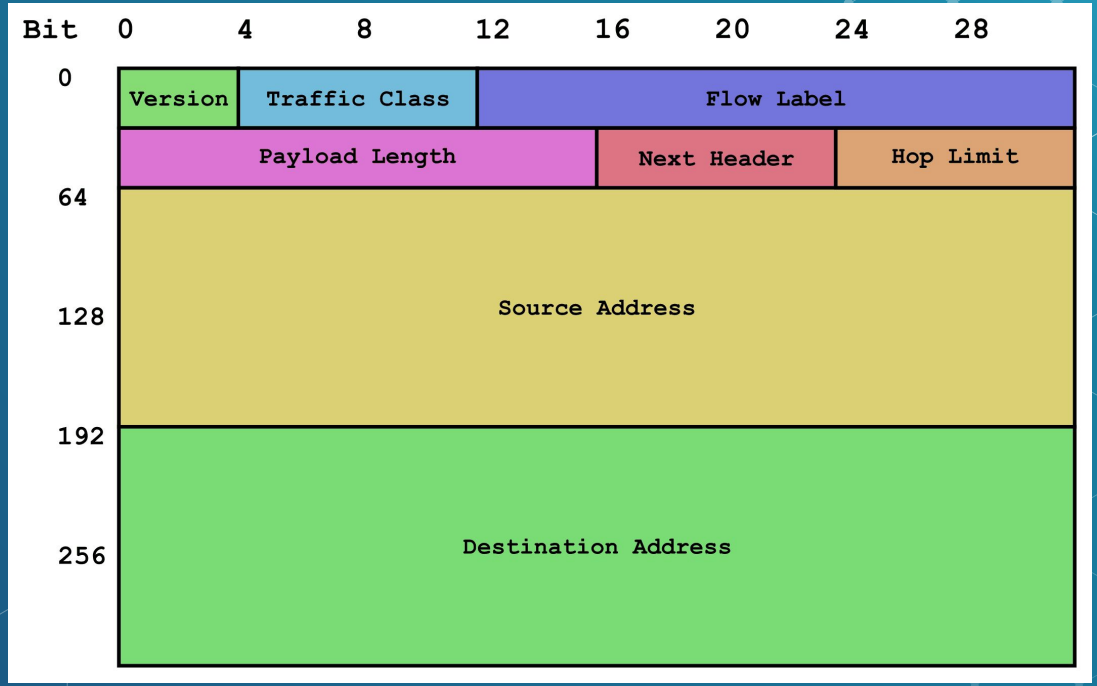


Image from https://networkel.com/ipv6-overview-communication-types/

What kind of DDoS? L4. TCP?

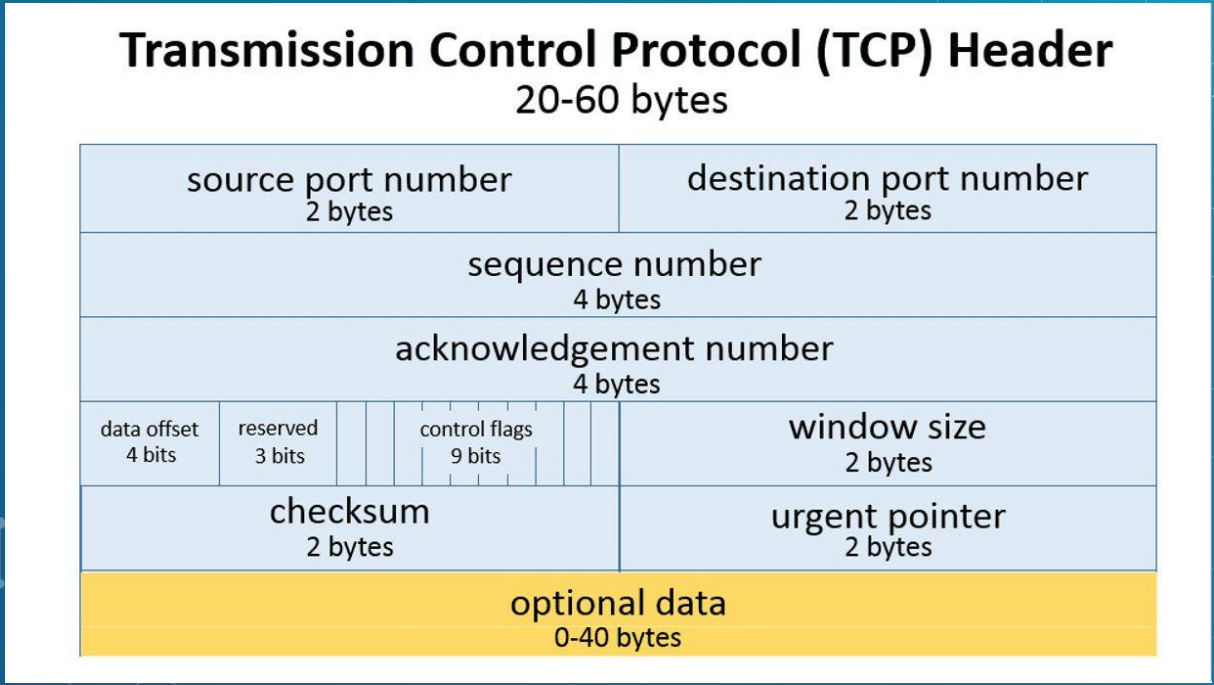
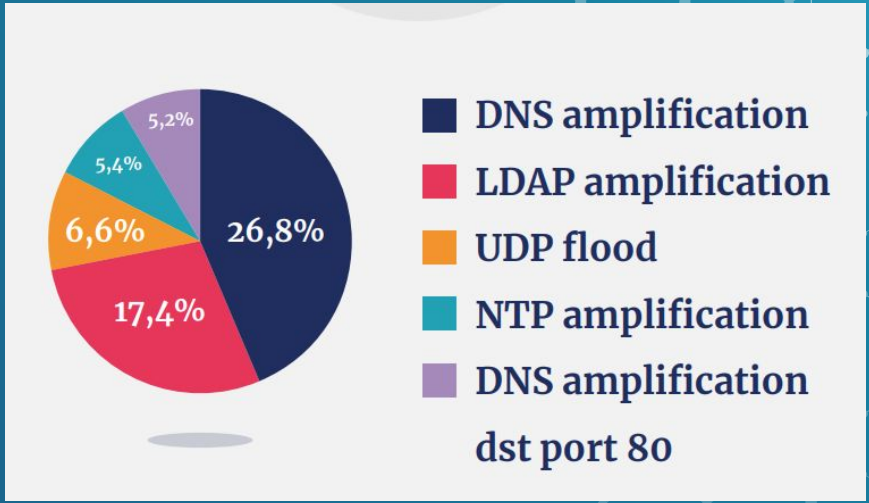


Image from https://www.lifewire.com/tcp-headers-and-udp-headers-explained-817970

What kind of DDoS? L3 and L4

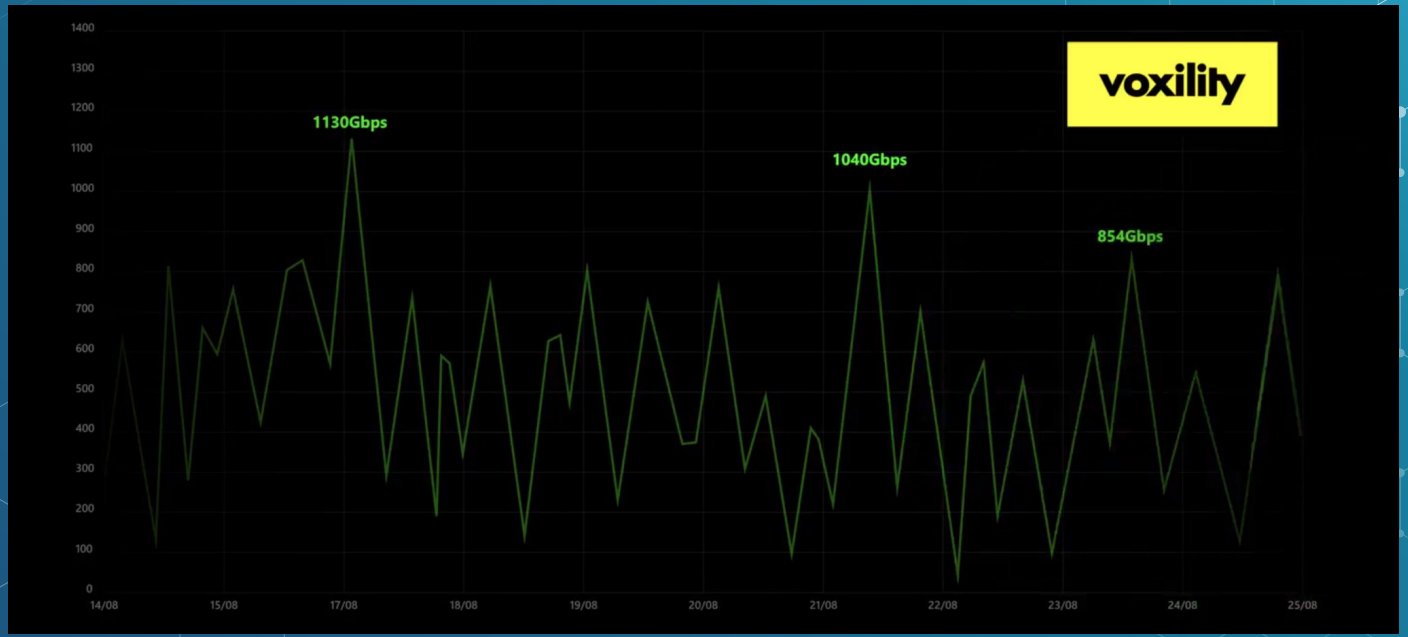
- TCP flag flood (i.e. SYN, ACK flood)
- UDP flood
- GRE flood
- UDP amplification (DNS, NTP, SSDP, SNMP)
- Fragmentation attack
- Spoofed source attacks

What is the DDoS weather?



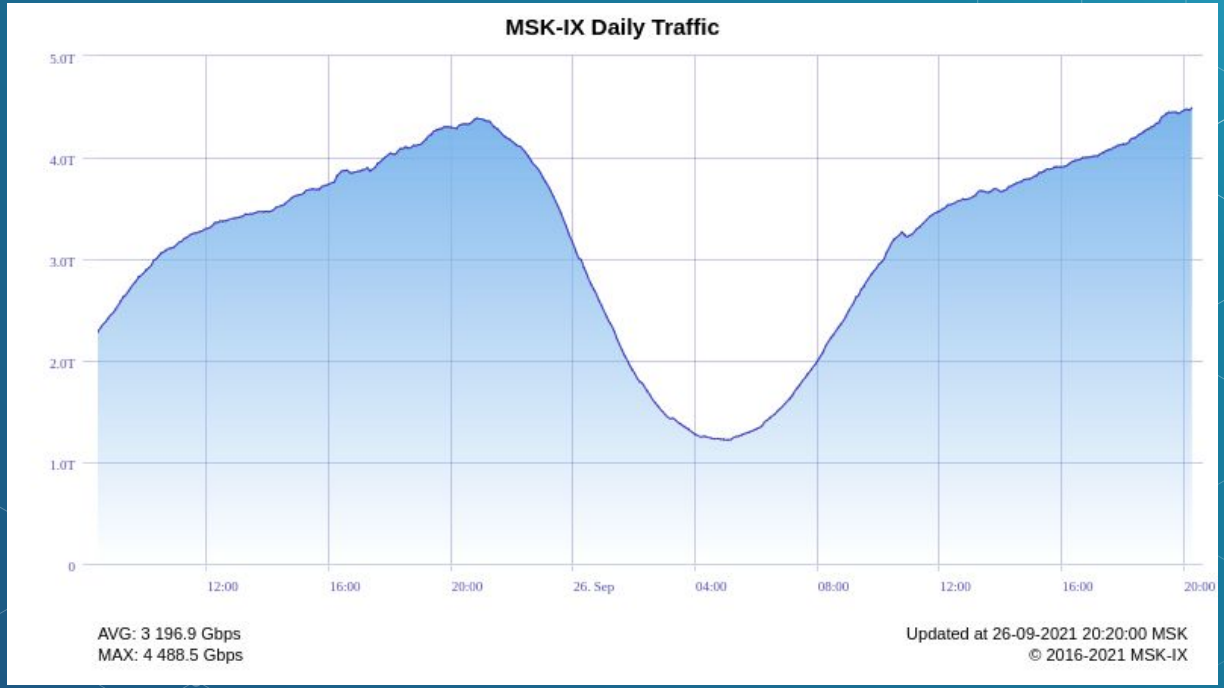
Data provided by The Dutch National Scrubbing Center (NaWas)

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

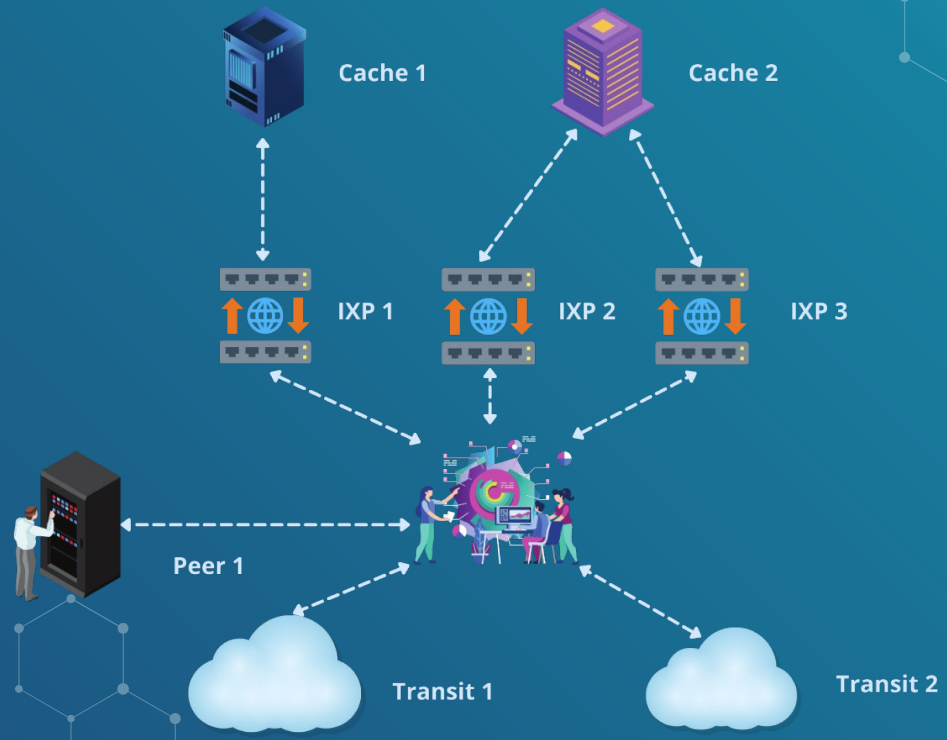
What about current capacity of MSK-IX?

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

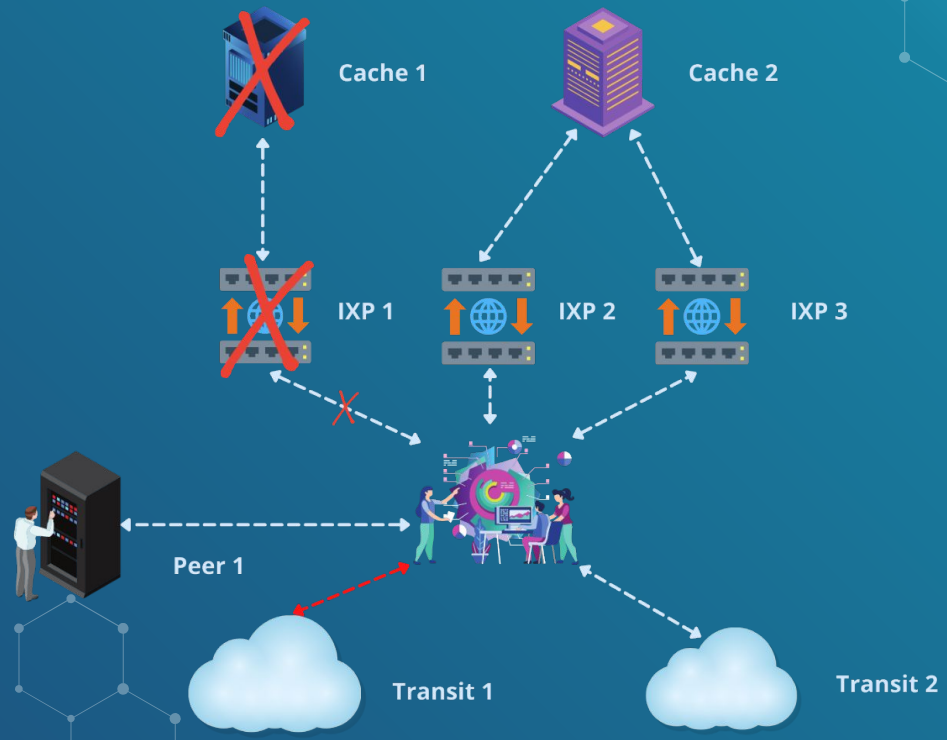
Data provided by MSK-IX

What is the problem?

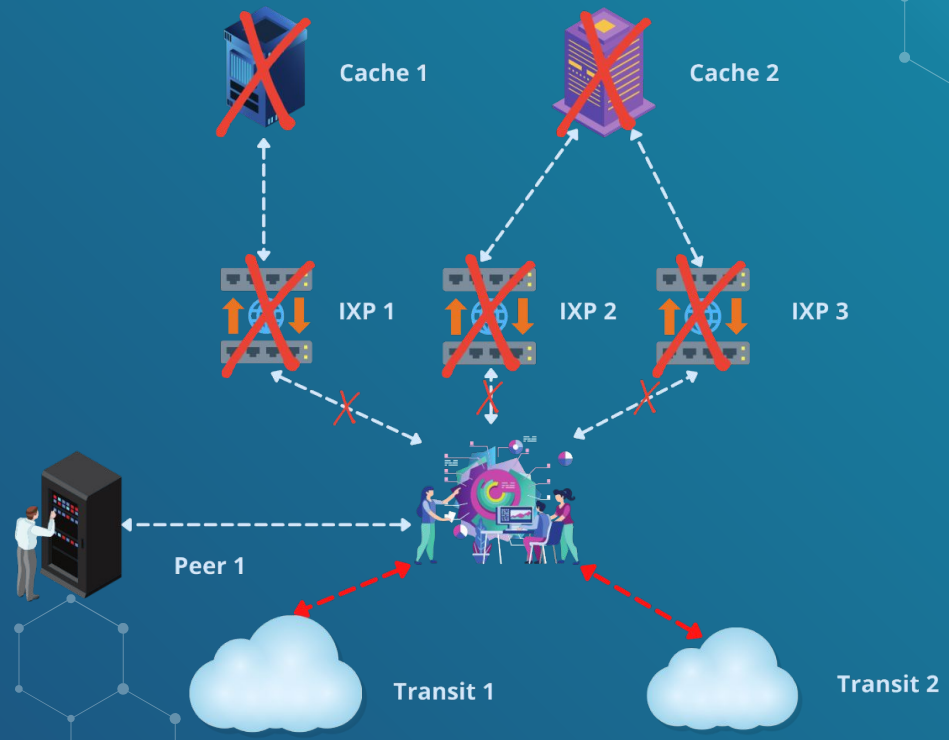
What is the common ISP setup?



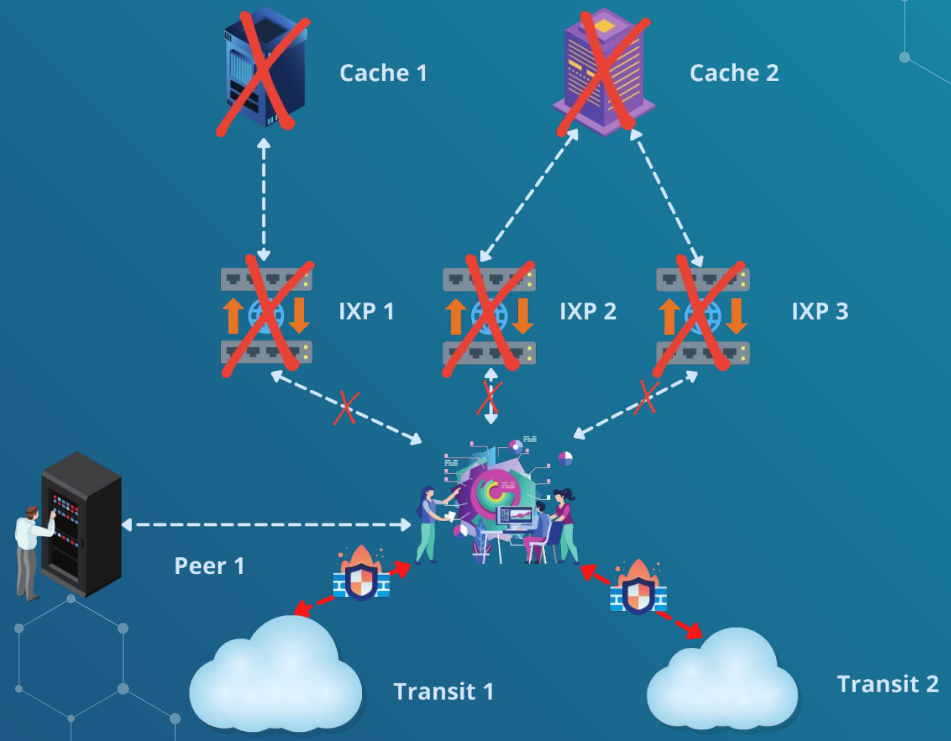
What can be done to stop an attack from IXP?



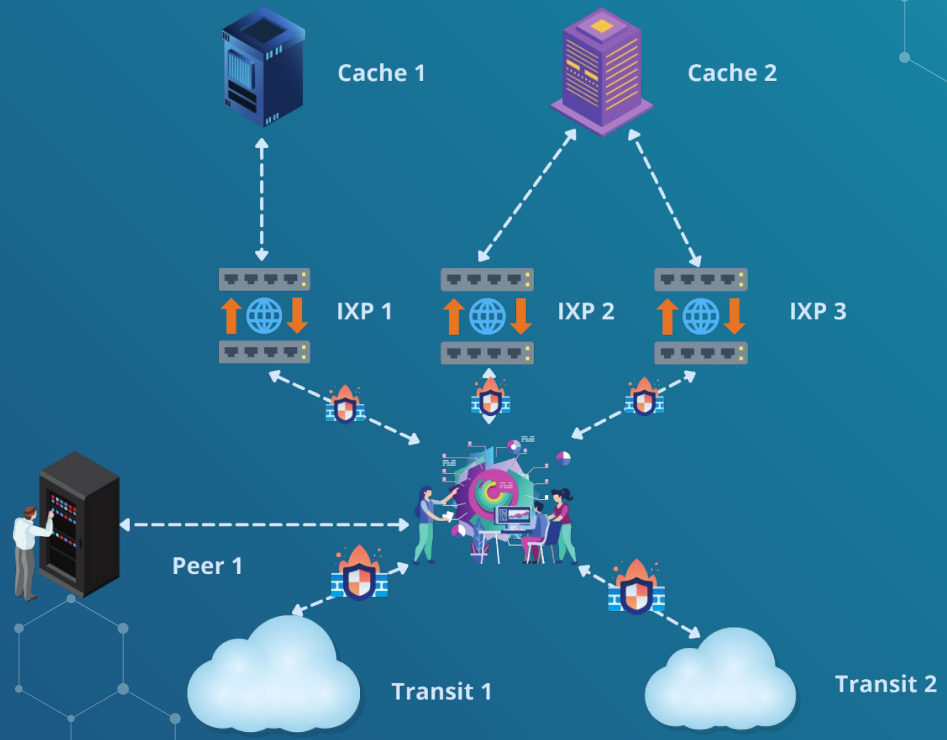
What can be done to stop an attack from IXPs?



What is the most secure configuration now?



What is the best configuration?



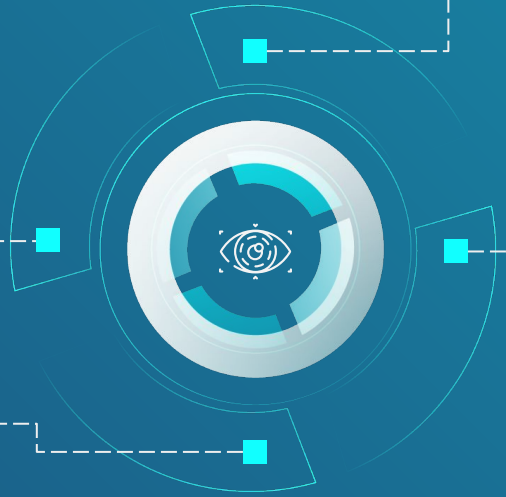
Traffic telemetry at IXP: sFlow

Very small / no delay

sFlow agents do not implement aggregation and they keep traffic only for very short period of time

Small CPU overheader

sFlow does not implement any kind of aggregation and does not need very efficient memory for flow tables



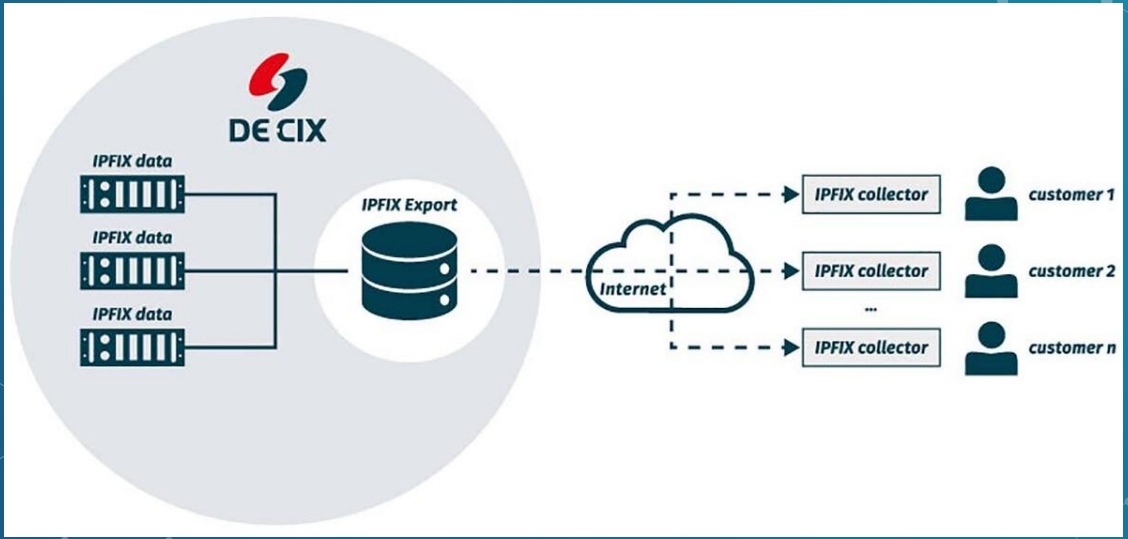
Keeps 60+ bytes from packet

Provides such important flags as TTL and fragmentation fields accompanied by first bytes of payload

Simple encoding protocol

Sampling rate is encoded directly in each packet, packet headers exported as-is without encoding

Traffic telemetry: sharing is caring



FastNetMon Community: features

- Supports all types of volumetric attacks
- Does not require changes in your network
- Complete automation
- Lightning fast detection
- Software only solution
- BGP integration
- Support almost all possible traffic capture engines (including sFlow)

FastNetMon: users

FastNetMon Community: platforms

- Debian 8, 9, 10
- Ubuntu 16.04, 18.04, 20.04
- RHEL 6, 7, 8
- AlmaLinux, Rocky Linux 8
- CentOS 6, 7, 8
- FreeBSD 9, 10, 11 (ports)
- Cumulus Linux
- VyOS (bundled)

FastNetMon: vendors

FastNetMon: attack detection time

- 2 seconds with mirror
- 4 seconds with sFlow
- 10-30 seconds with NetFlow/IPFIX

FastNetMon: traffic capture backends

- sFlow v5 (switches, routers)
- Netflow v5, v9, v10 (IPFIX), jFlow, cFlow (routers)
- SPAN/MIRROR (1GE, 10GE, 40GE)

FastNetMon: scalability

- sFlow v5 – 1.2 Tbps*
- NetFlow – 2.2 Tbps*
- Mirror/SPAN – 80 GE*

All numbers are for single server

FastNetMon: attack actions

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

FastNetMon: fast deployment

- Works on any VM or physical server
- Less then 15 minutes to install and configure FastNetMon on new server!
- Learns almost all configuration automatically!

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:

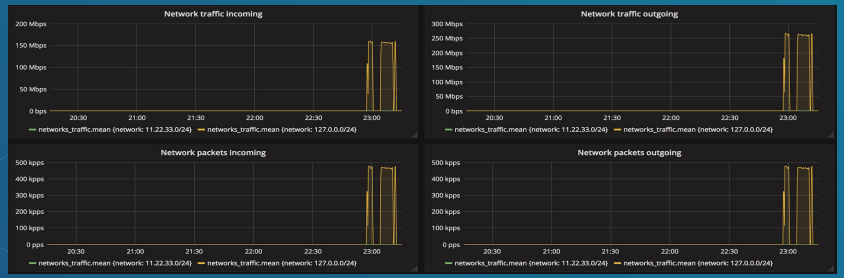
- Using total traffic
- Using total pps rate
- Per protocol

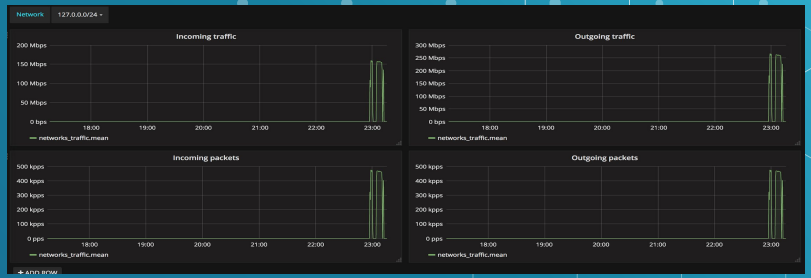
FastNetMon: attack reports

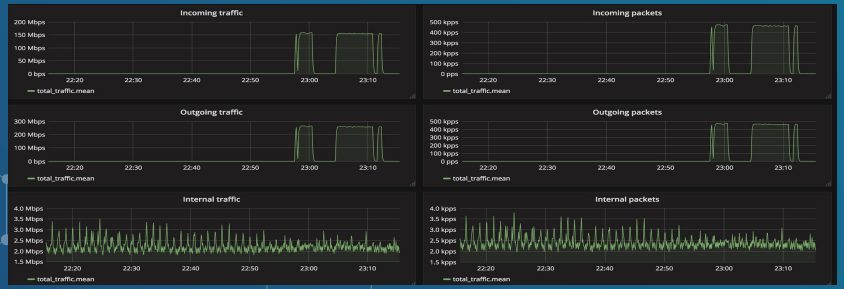
IP: 10.10.10.221Attack type: syn_flood
Initial attack power: 546475 packets per second
Peak attack power: 546475 packets per second
Attack direction: incoming
Attack protocol: tcp
Total incoming traffic: 245 mbps
Total outgoing traffic: 0 mbps
Total incoming pps: 99059 packets per second
Total outgoing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

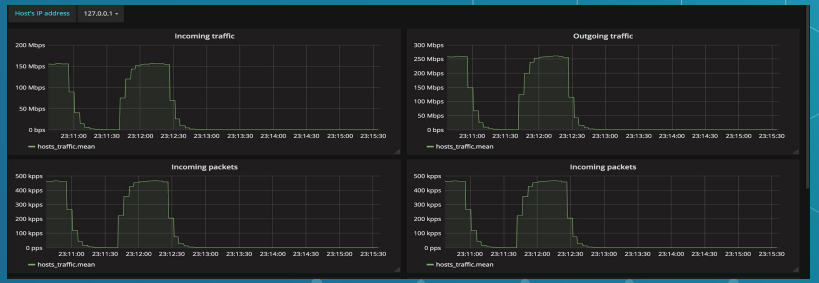
IP: 10.10.10.221Attack type: syn_flood
Initial attack power: 546475 packets per second
Peak attack power: 546475 packets per second
Attack direction: incoming
Attack protocol: tcp
Total incoming traffic: 245 mbps
Total outgoing traffic: 0 mbps
Total incoming pps: 99059 packets per second
Total outgoing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

```
#!/usr/bin/env bash

# Save it to: /usr/local/bin/notify_about_attack.sh

email_notify="noc@please-deploy-ipv6.co.uk"

if [ "$4" = "ban" ]; then
    cat | mail -s "FastNetMon Guard: IP $1 blocked because $2 attack with power $3 pps" $email_notify;
    # You can add ban code here!
    exit 0
fi

if [ "$4" = "unban" ]; then
    # No details on stdin here
    # Unban actions if used
    exit 0
fi
```

FastNetMon: default configuration

```
ban_for_pps = on
ban_for_bandwidth = on
ban_for_flows = off
threshold_pps = 20000
threshold_mbps = 1000
threshold_flows = 3500
threshold_tcp_mbps = 100000
threshold_udp_mbps = 100000
threshold_icmp_mbps = 100000
threshold_tcp_pps = 100000
threshold_udp_pps = 100000
threshold_icmp_pps = 100000
ban_for_tcp_bandwidth = off
ban_for_udp_bandwidth = off
ban_for_icmp_bandwidth = off
ban_for_tcp_pps = off
ban_for_udp_pps = off
ban_for_icmp_pps = off
```

```
hostgroup =
my_hosts:10.10.10.221/32,10.10.10.222/32

my_hosts_enable_ban = off

my_hosts_ban_for_pps = off
my_hosts_ban_for_bandwidth = off
my_hosts_ban_for_flows = off

my_hosts_threshold_pps = 20000
my_hosts_threshold_mbps = 1000
my_hosts_threshold_flows = 3500
```

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