FastNetMon Community: open source tool for DDoS Detection

Hello, I'm Pavel

I'm a software engineer and entrepreneur with passion in computer networks and founder of FastNetMon LTD, London

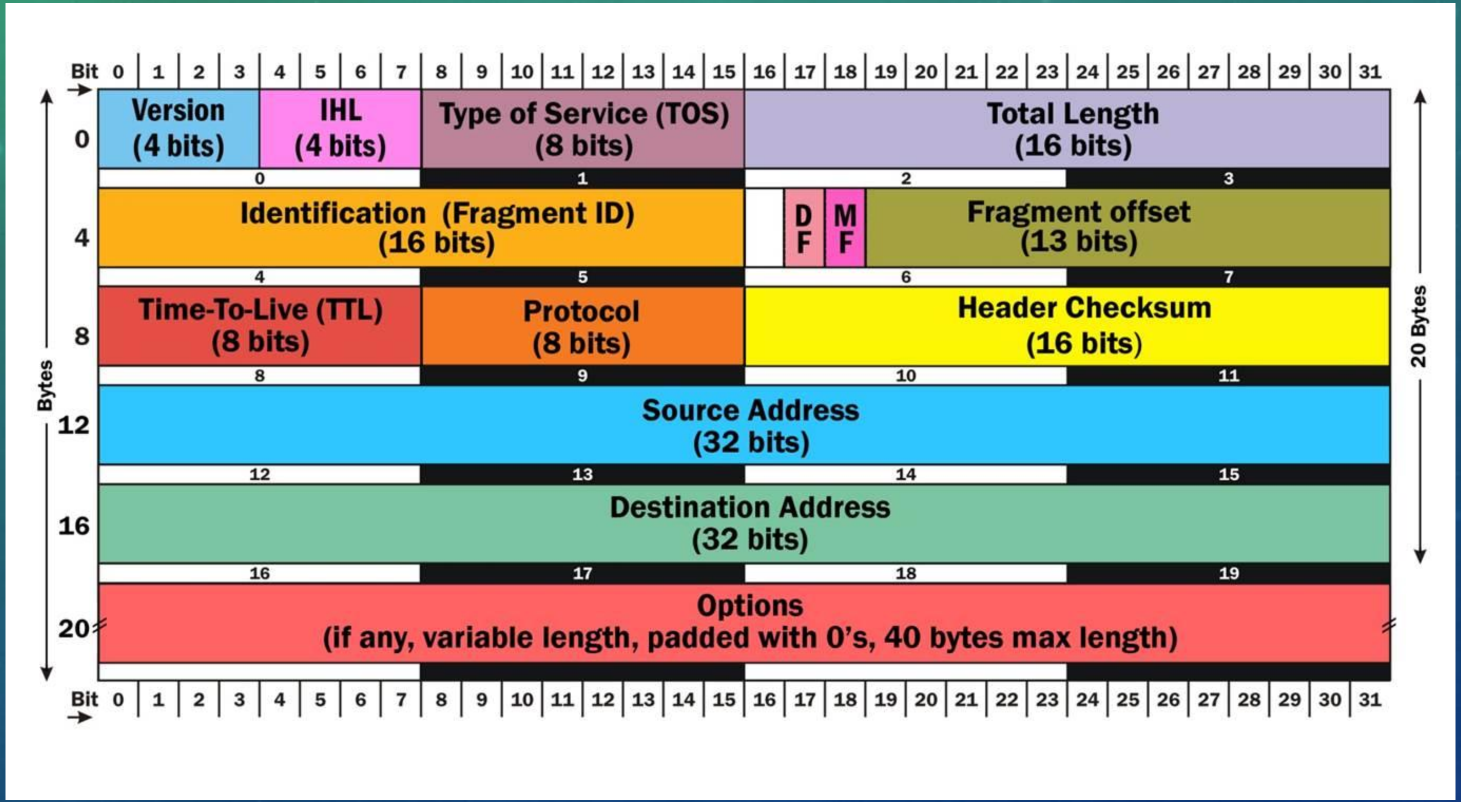
Career path:

- Domain name registrar
- Cloud compute provider
- IXP
- Cloudflare
- FastNetMon

What is FastNetMon Community?

It's a cross platform (Linux, FreeBSD, macOS) application for DDoS detection implemented using the C++ 17 language and licensed under GPLv2

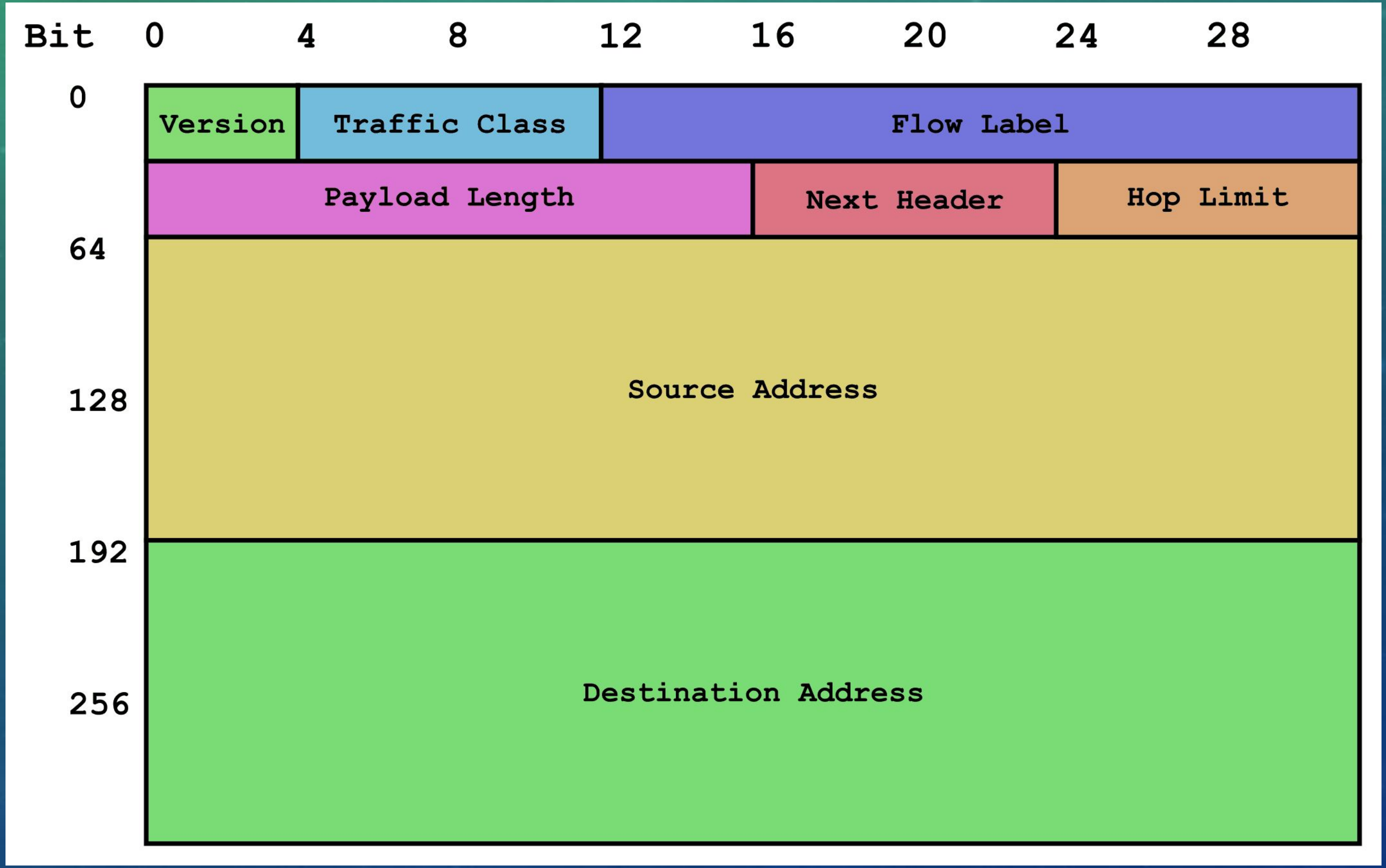
What Kind of DDoS? L3. IPv4



0	Version (4 bits)	IHL (4 bits)	Type of Service (TOS) (8 bits)	Total Length (16 bits)	
4	Identification (Fragment ID) (16 bits)		DF	MF	Fragment offset (13 bits)
8	Time-To-Live (TTL) (8 bits)	Protocol (8 bits)	Header Checksum (16 bits)		
12	Source Address (32 bits)				
16	Destination Address (32 bits)				
20	Options (if any, variable length, padded with 0's, 40 bytes max length)				

Bit 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Bytes
20 Bytes
0 1 2 3
4 5 6 7
8 9 10 11
12 13 14 15
16 17 18 19

What Kind of DDoS? L3. IPv6



Bit 0 4 8 12 16 20 24 28

0

Version

Traffic Class

Flow Label

Payload Length

Next Header

Hop Limit

64

128

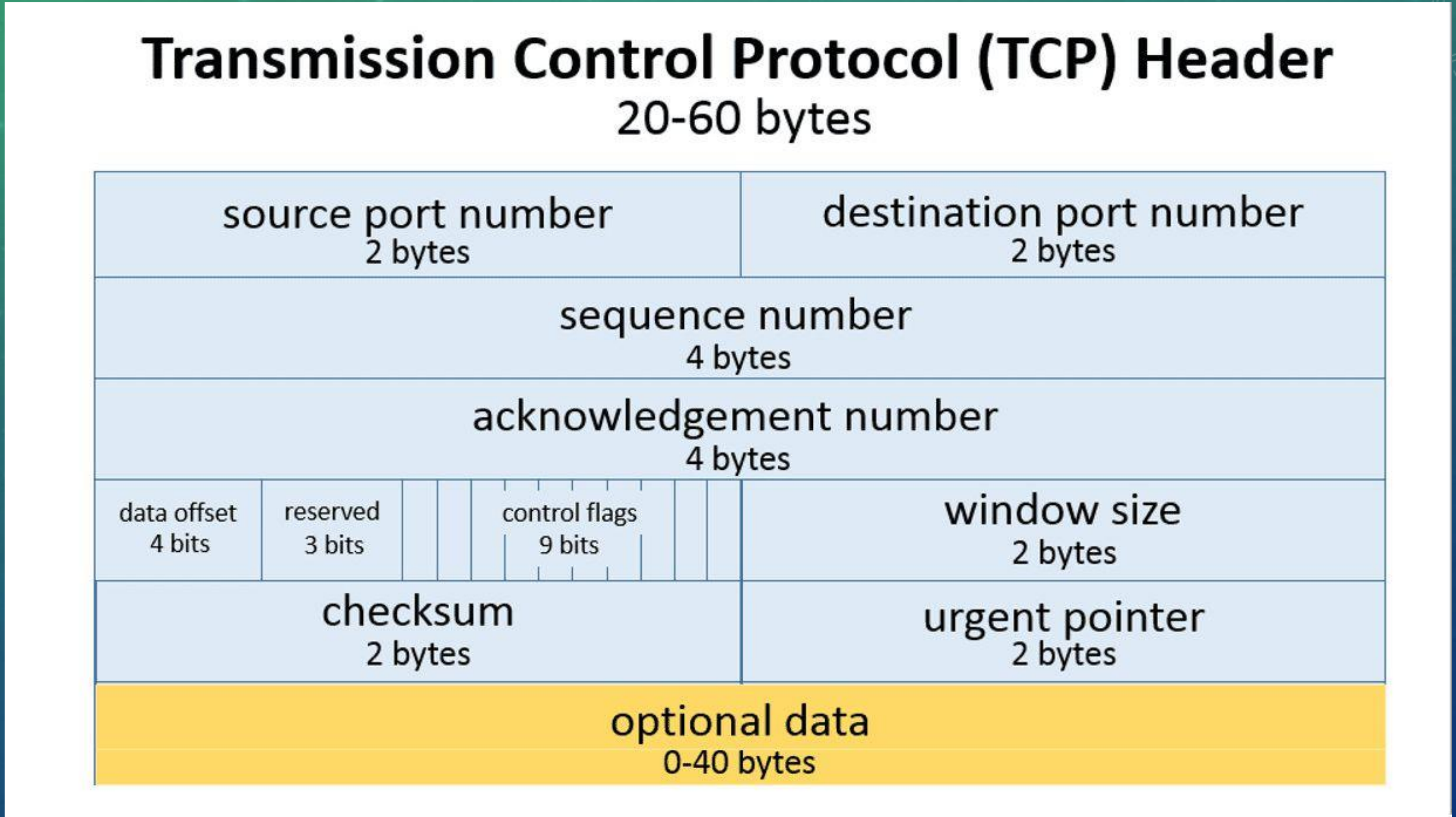
Source Address

192

256

Destination Address

What Kind of DDoS? L4. TCP



Transmission Control Protocol (TCP) Header

20-60 bytes

source port number
2 bytes

destination port number
2 bytes

sequence number
4 bytes

acknowledgement number
4 bytes

data offset
4 bits

reserved
3 bits

control flags
9 bits

window size
2 bytes

checksum
2 bytes

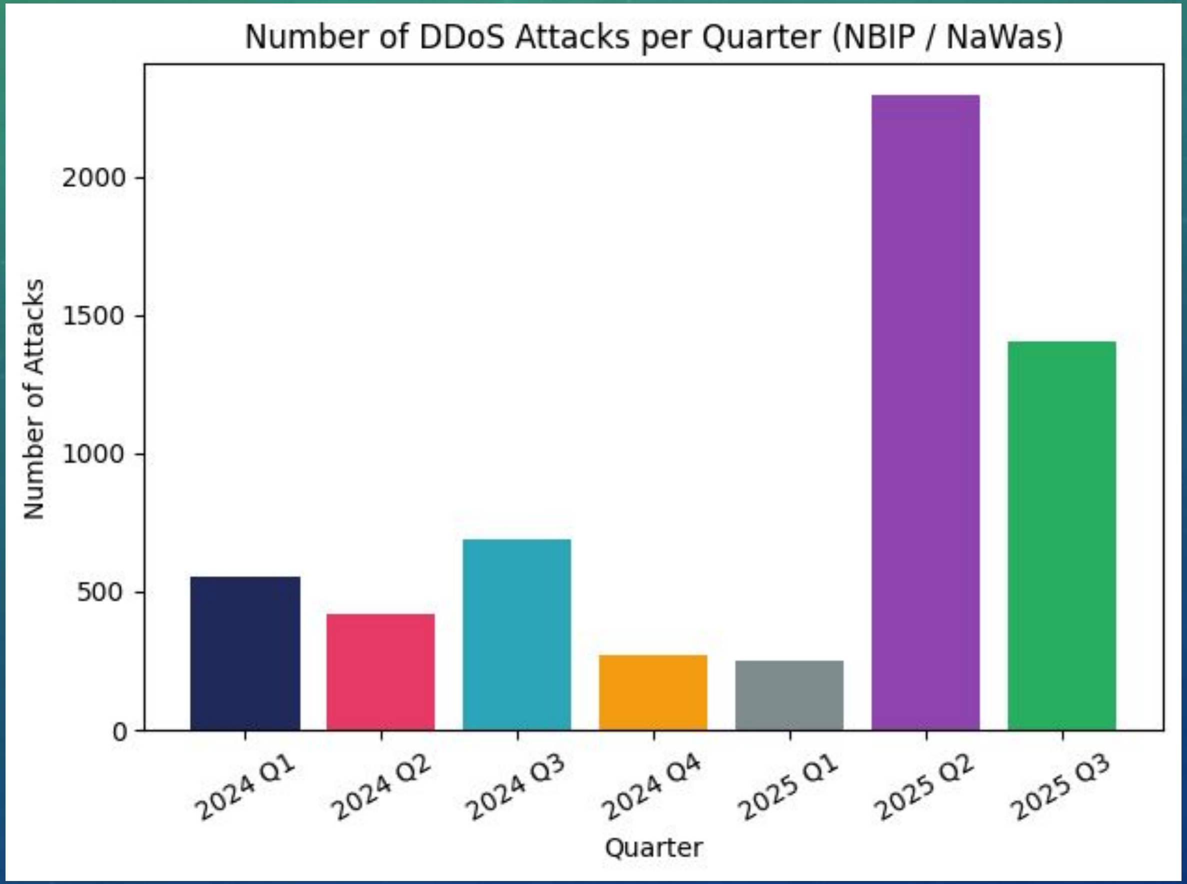
urgent pointer
2 bytes

optional data
0-40 bytes

What Kind of DDoS? L3 and L4

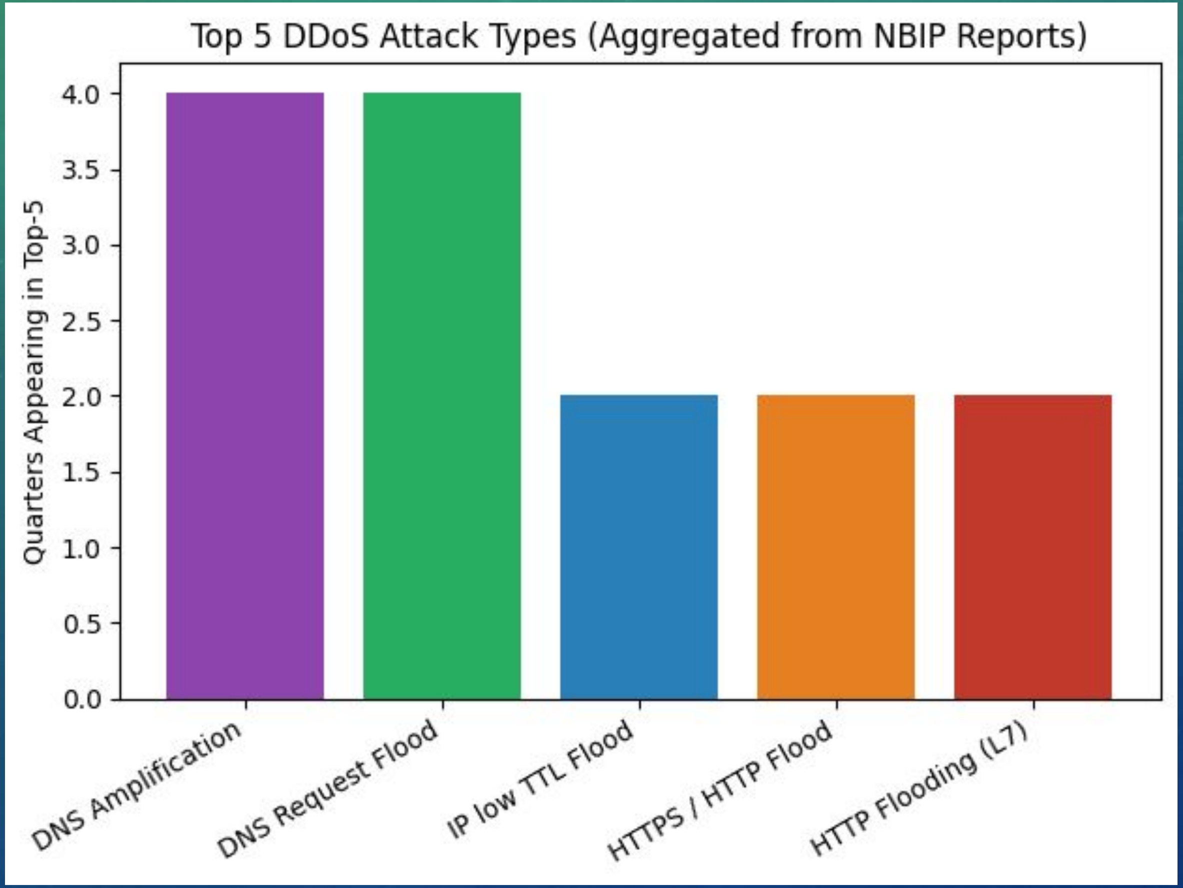
- TCP flag flood (i.e. SYN, ACK flood)
- UDP flood
- GRE flood
- UDP amplification (DNS, NTP, SSDP, SNMP)
- Fragmentation attack
- Spoofed source attacks

What is the DDoS Weather?



Data provided by The Dutch National Scrubbing Center (NaWas)

What is the DDoS Weather?



Data provided by The Dutch National Scrubbing Center (NaWas)

Supported Vendors

ARISTA

NOKIA

JUNIPER NETWORKS

HUAWEI

A10

radware

hp

Extreme

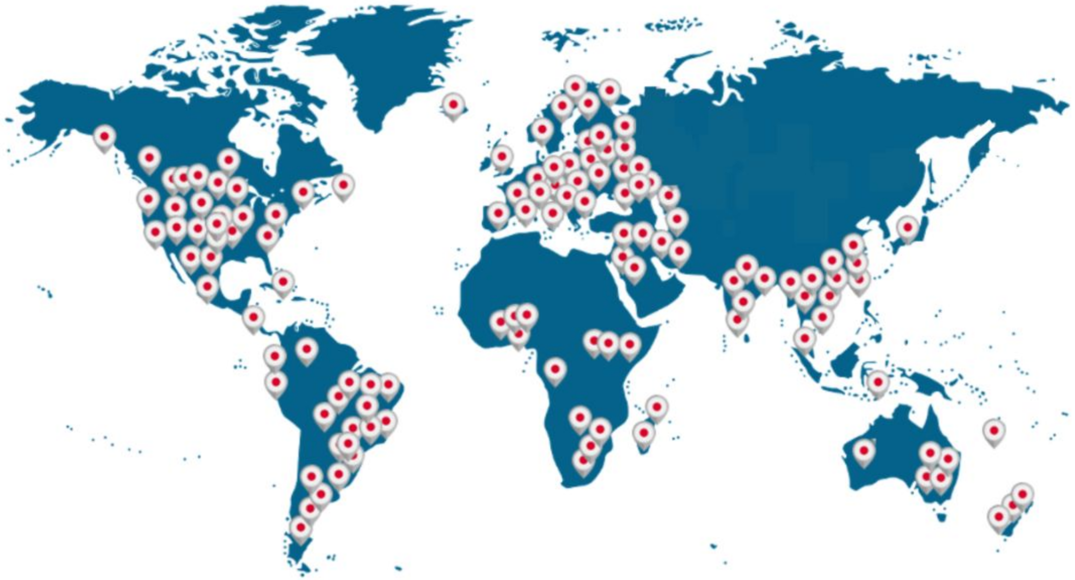
Connect Beyond the Network

Edge-corE NETWORKS

CISCO

DELL

FastNetMon Users



Key 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

Supported Distributions

- Debian 8, 9, 10, 11, 12
- Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04
- RHEL 6, 7, 8, 9
- AlmaLinux, Rocky Linux 8, 9
- CentOS 6, 7, 8
- FreeBSD 9, 10, 11 (ports)
- Cumulus Linux
- VyOS (bundled)

What is the best way to install it?

Ubuntu 24.04 or newer:	apt install fastnetmon
Debian 12 or newer:	apt install fastnetmon
Fedora 35 or newer:	dnf install fastnetmon
RHEL 9 or newer, EPEL:	dnf install fastnetmon
macOS, Homebrew:	brew install fastnetmon
FreeBSD:	pkg install fastnetmon

What is the best way to install the latest version?

```
wget https://install.fastnetmon.com/installer
sudo chmod +x installer
sudo ./installer –install_community_edition
```

Lightning Fast Attack Detection

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

Traffic Capture Backends

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

Detected Attack Types

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

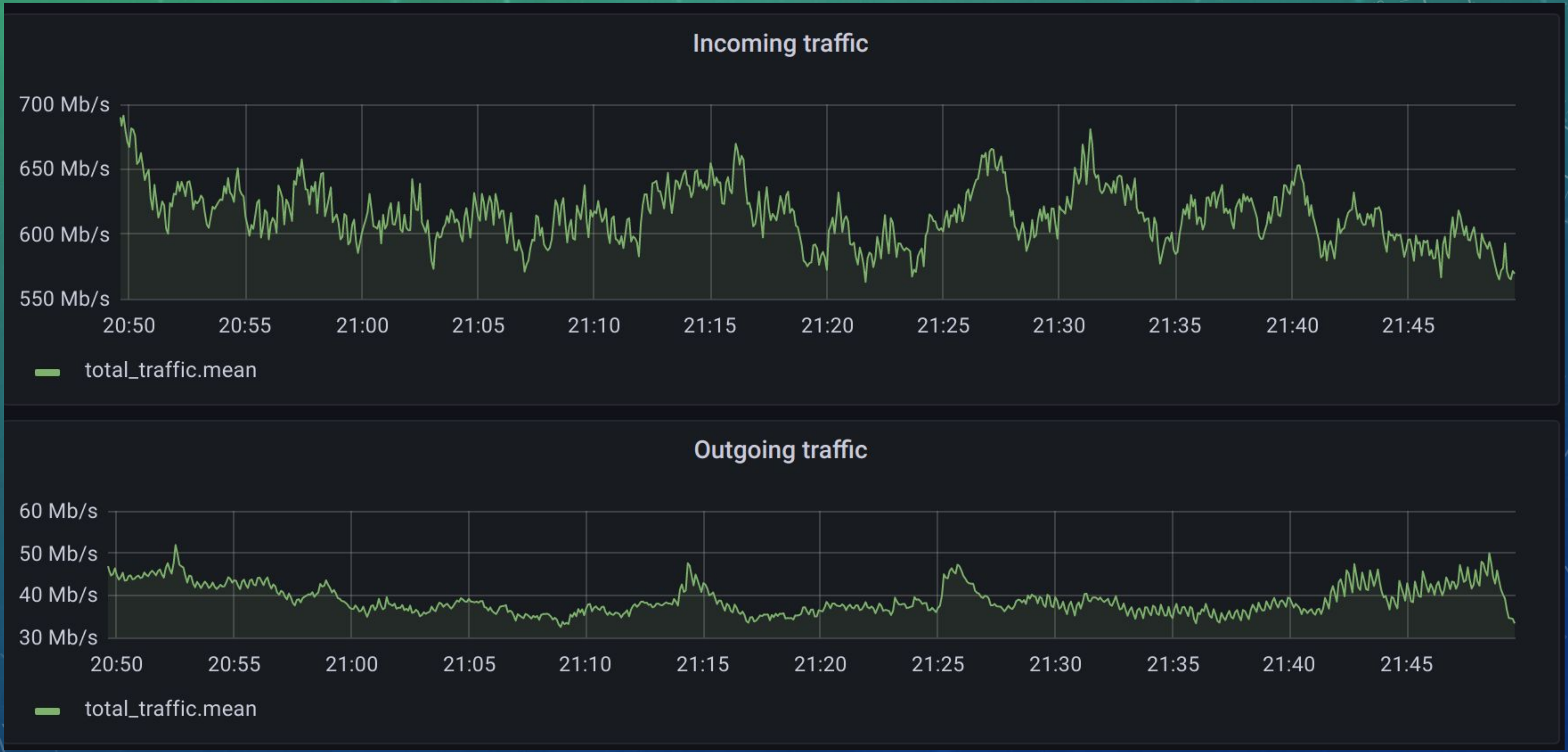
Lab Tested Scalability

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

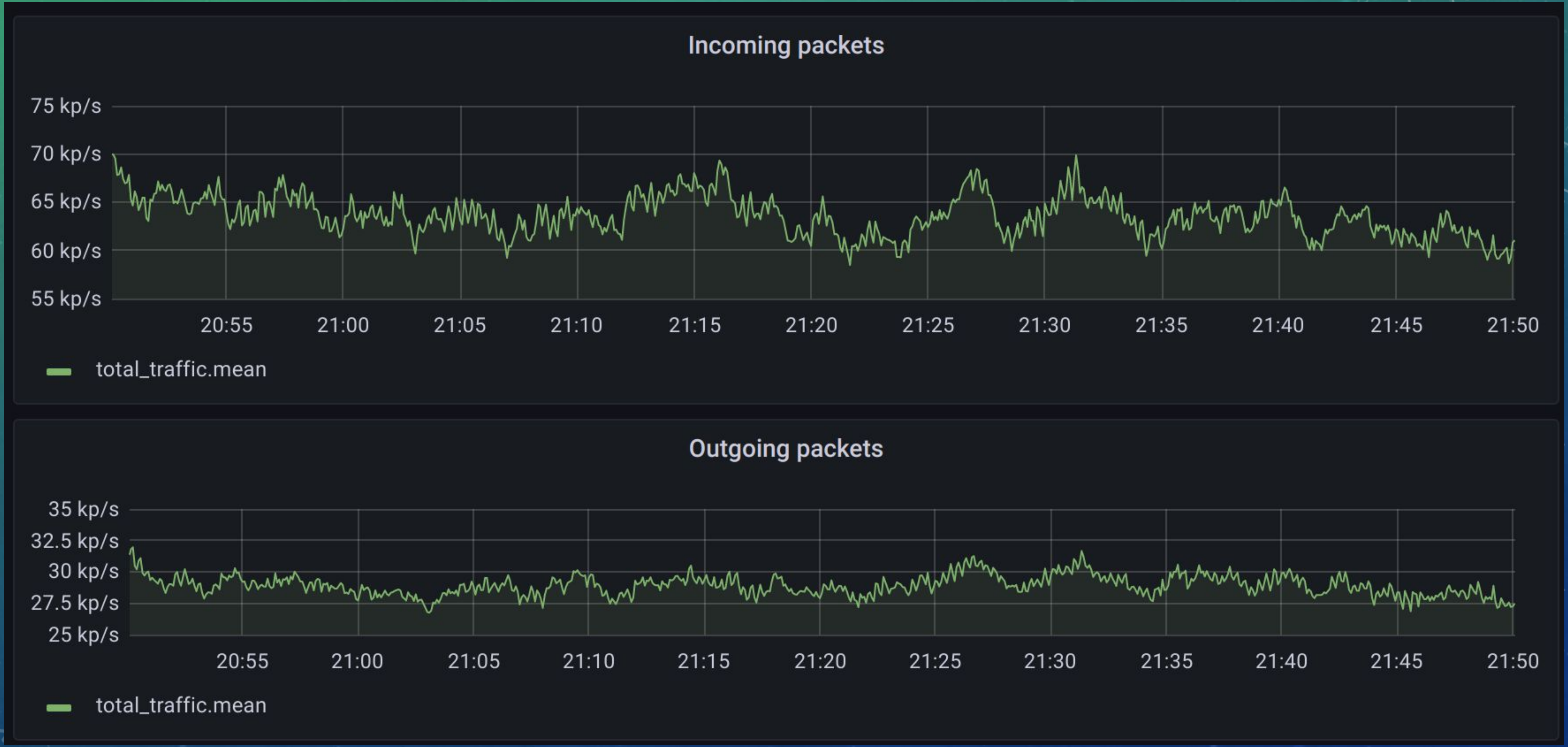
Attack Detection Actions

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

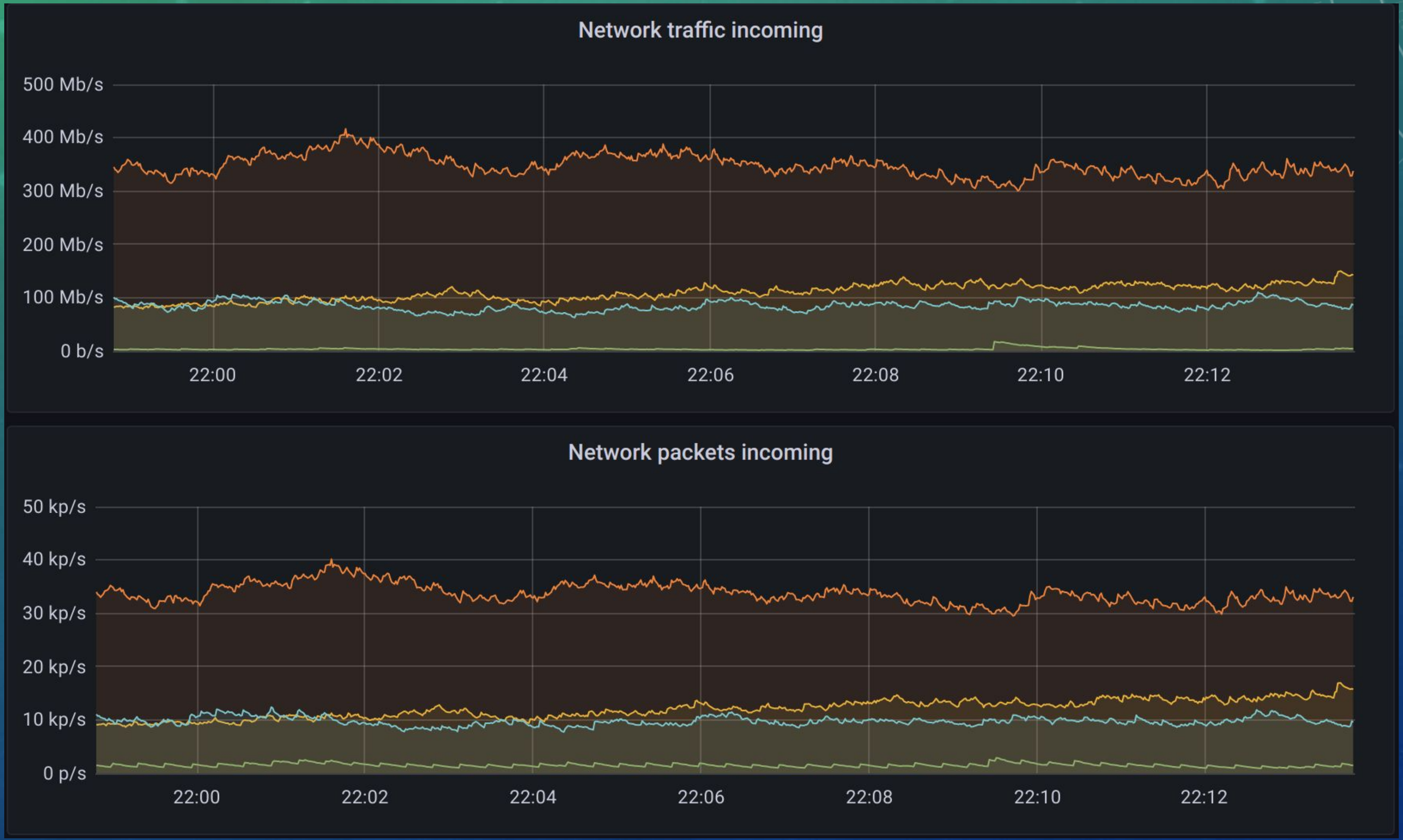
Total Incoming Traffic



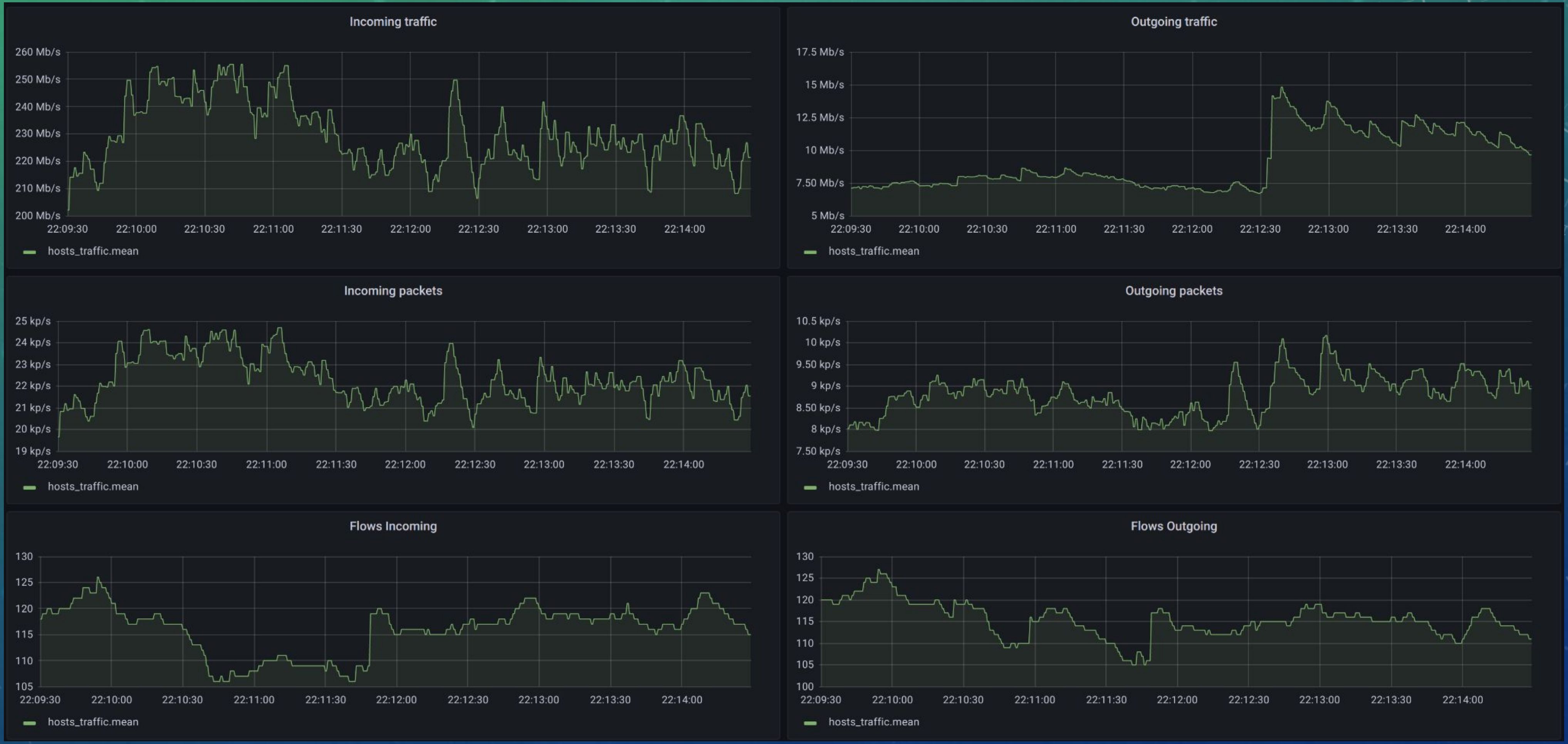
Total Outgoing Traffic



Per Network Traffic



Per Host Traffic



Very Fast Installation

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

Detection Logic

- Thresholds based on host's average traffic, /32 or /128

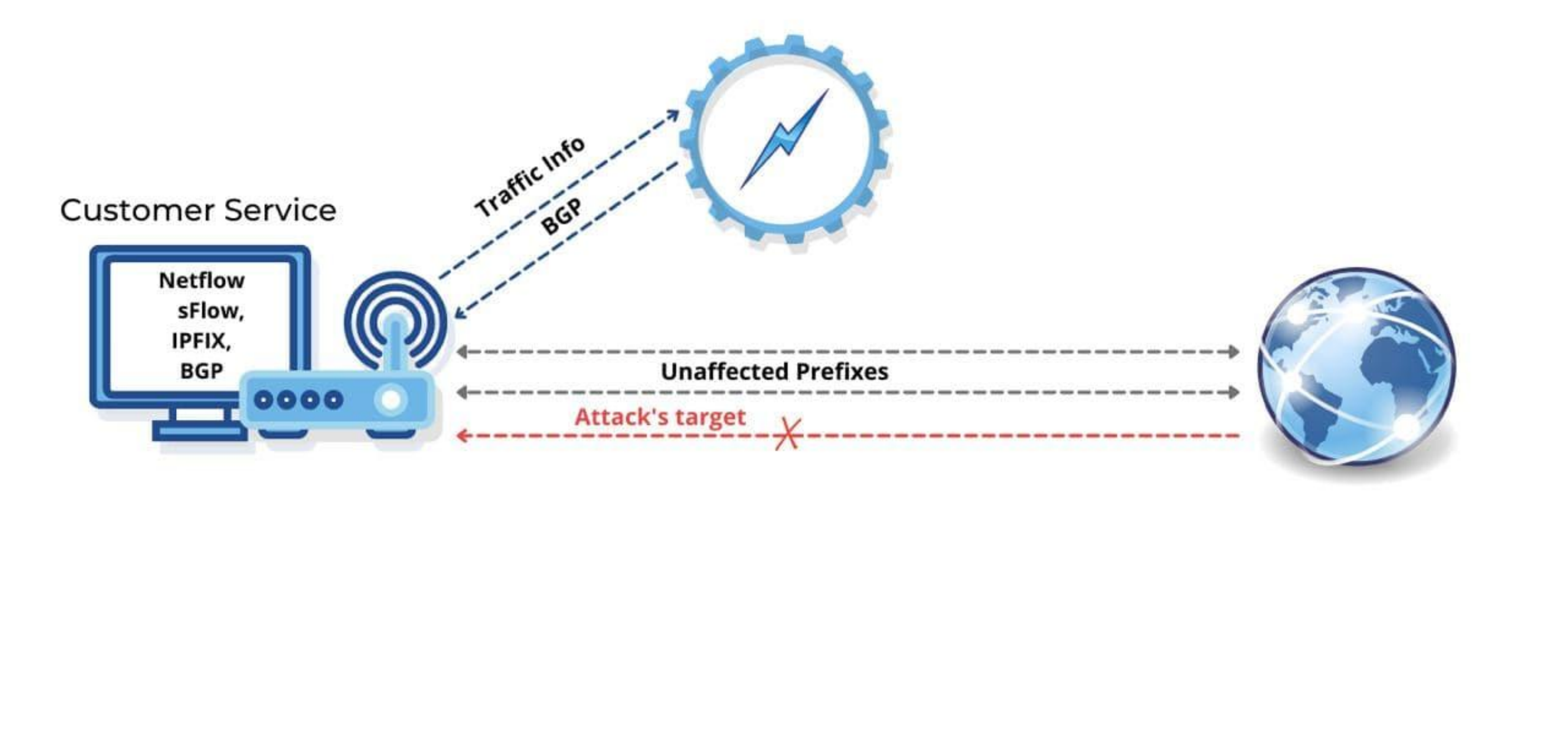
Supported Thresholds

- Packets / s
- Bits / s
- Flows / s
- TCP bits / s
- UDP bits / s
- ICMP bits / s
- TCP packets / s
- UDP packets / s
- ICMP packets / s

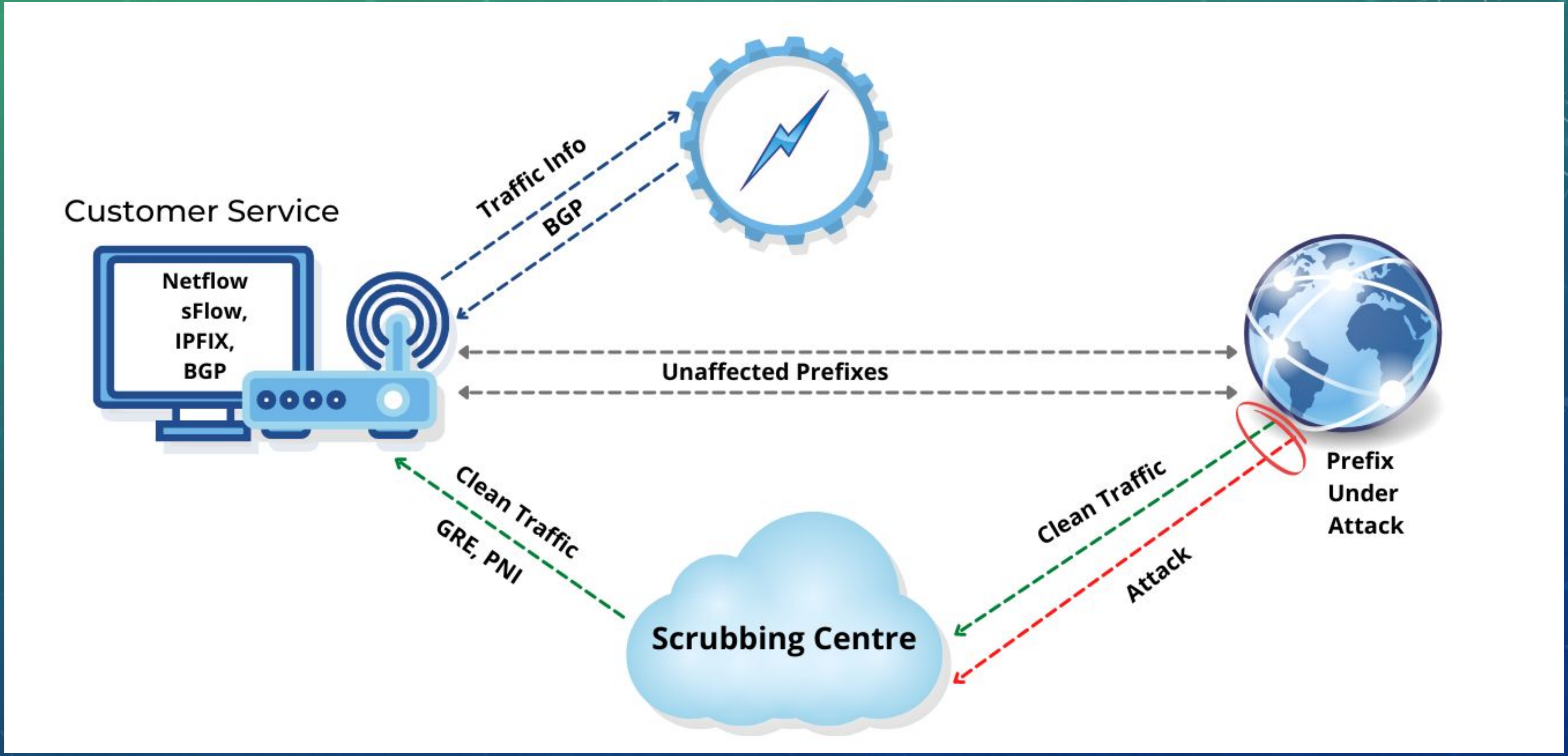
Between Cloud and On Premise

- You could use FastNetMon together with precise filtering hardware (Radware, A-10 Networks, Palo-Alto Networks)
- You could use FastNetMon with your favourite DDoS filtering cloud
- You could use FastNetMon to isolate attacked customer in special network using BGP diversion

RTBH Automation



Cloud Scrubbing Diversion



Rich 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
```

```
Incoming ip fragmented traffic: 250 mbps
Outgoing ip fragmented traffic: 0 mbps
Incoming ip fragmented pps: 546475 packets per second
Outgoing ip fragmented pps: 0 packets per second
Incoming tcp traffic: 250 mbps
Outgoing tcp traffic: 0 mbps
Incoming tcp pps: 546475 packets per second
Outgoing tcp pps: 0 packets per second
Incoming syn tcp traffic: 250 mbps
Outgoing syn tcp traffic: 0 mbps
Incoming syn tcp pps: 546475 packets per second
Outgoing syn tcp pps: 0 packets per second
Incoming udp traffic: 0 mbps
Outgoing udp traffic: 0 mbps
Incoming udp pps: 0 packets per second
Outgoing udp pps: 0 packets per second
Incoming icmp traffic: 0 mbps
Outgoing icmp traffic: 0 mbps
```

Callback Scripts

```
#!/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
```

How to reach me?

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

Community

- Site: https://fastnetmon.com/guides/
- GitHub: https://github.com/pavel-odintsov/fastnetmon
- Discord: https://discord.fastnetmon.com/
- IRC: #fastnetmon at Libera Chat
- Telegram: https://t.me/fastnetmon
- Slack: https://slack.fastnetmon.com
- LinkedIN: https://www.linkedin.com/company/fastnetmon/
- Facebook: https://www.facebook.com/fastnetmon/
- Mail list: https://groups.google.com/forum/#!forum/fastnetmon

Thank you!