



# FastNetMon Community: open source tool for DDoS Detection



# Hello, I'm Pavel

I'm a software engineer with passion in computer networks and CTO / co-founder of FastNetMon LTD, London

Career path:

- Domain name registrar
- Cloud compute provider
- IXP
- Global CDN
- 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 is the best way to install it?

- Ubuntu 22.10 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
```



What can FastNetMon not do?

# FastNetMon cannot protect your website from attack

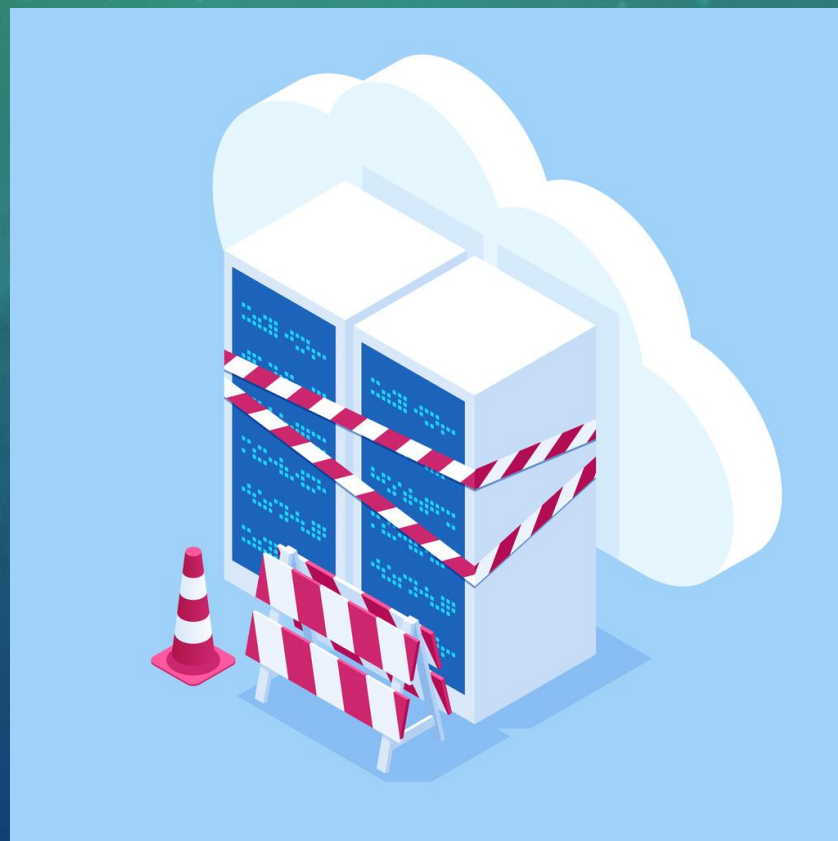


FastNetMon cannot protect your game console from attack



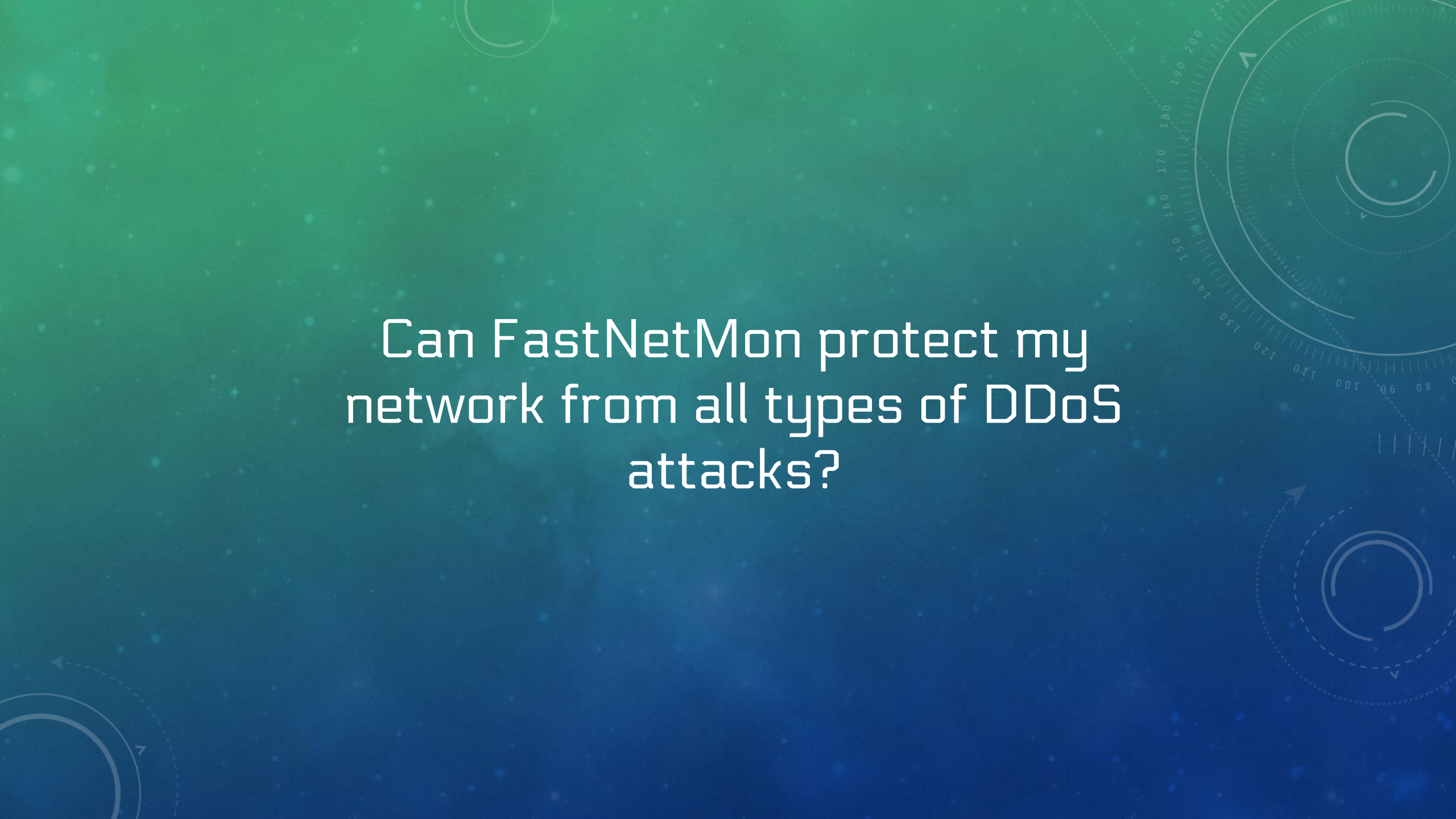


# FastNetMon cannot protect your managed cloud server from attack



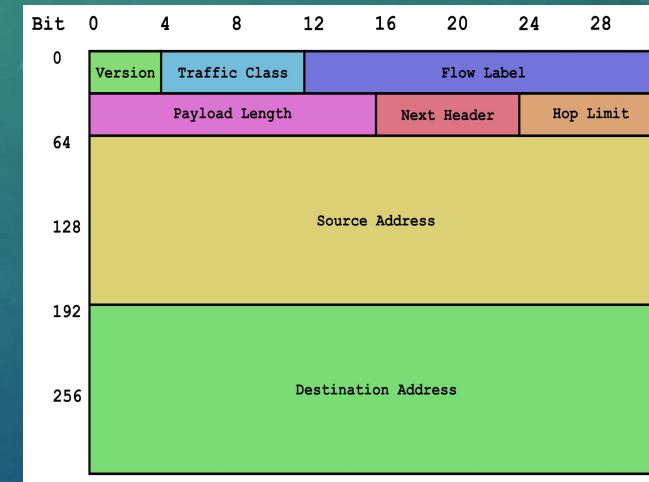
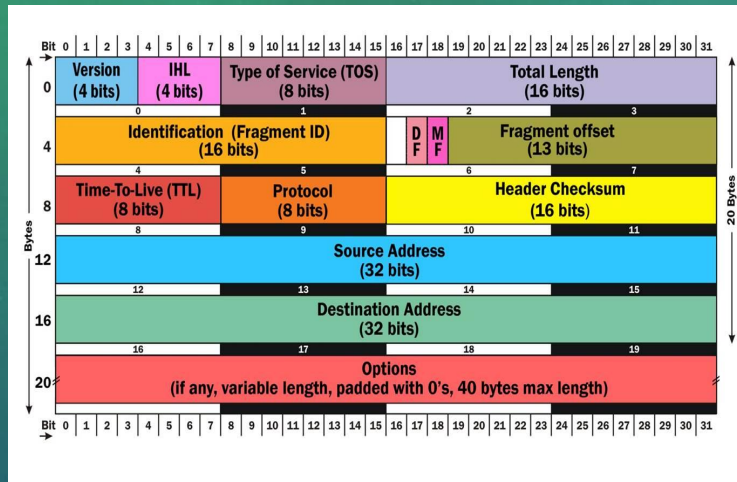
# FastNetMon can protect your network from DDoS attacks



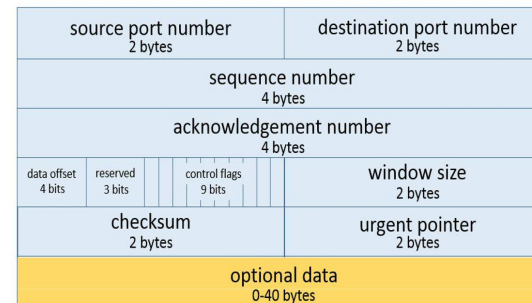


Can FastNetMon protect my  
network from all types of DDoS  
attacks?

# FastNetMon can help you with L3, L4 IPv4 and IPv6 volumetric attacks



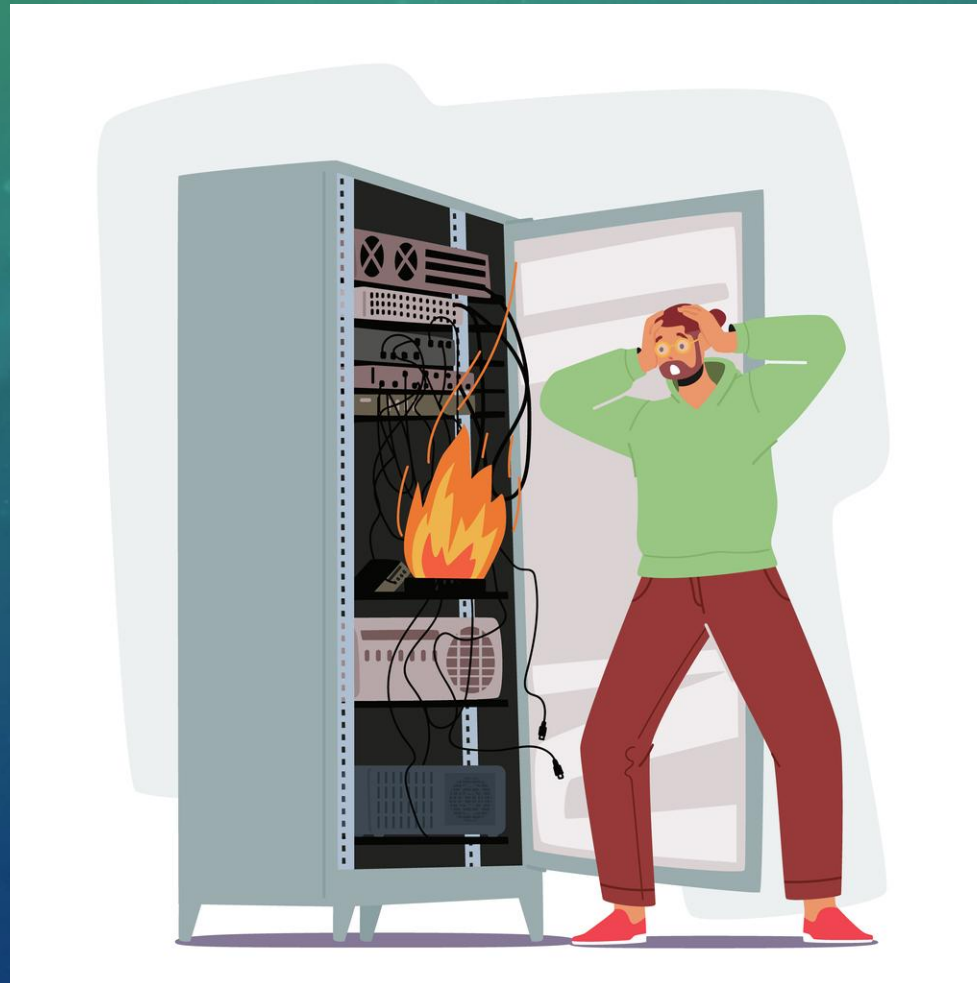
## Transmission Control Protocol (TCP) Header 20-60 bytes



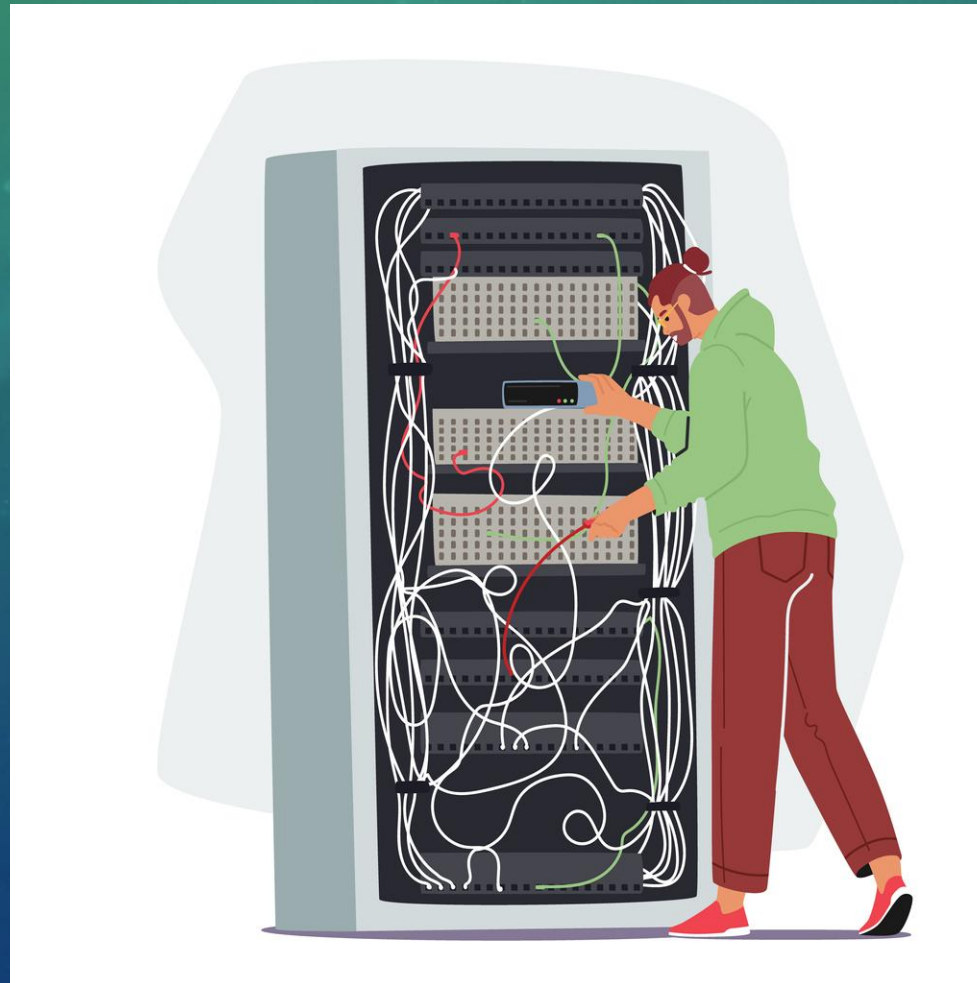


What is the very first step to do  
when you suspect a DDoS attack  
on your network?

This is clearly not a DDoS



This is clearly not a DDoS too

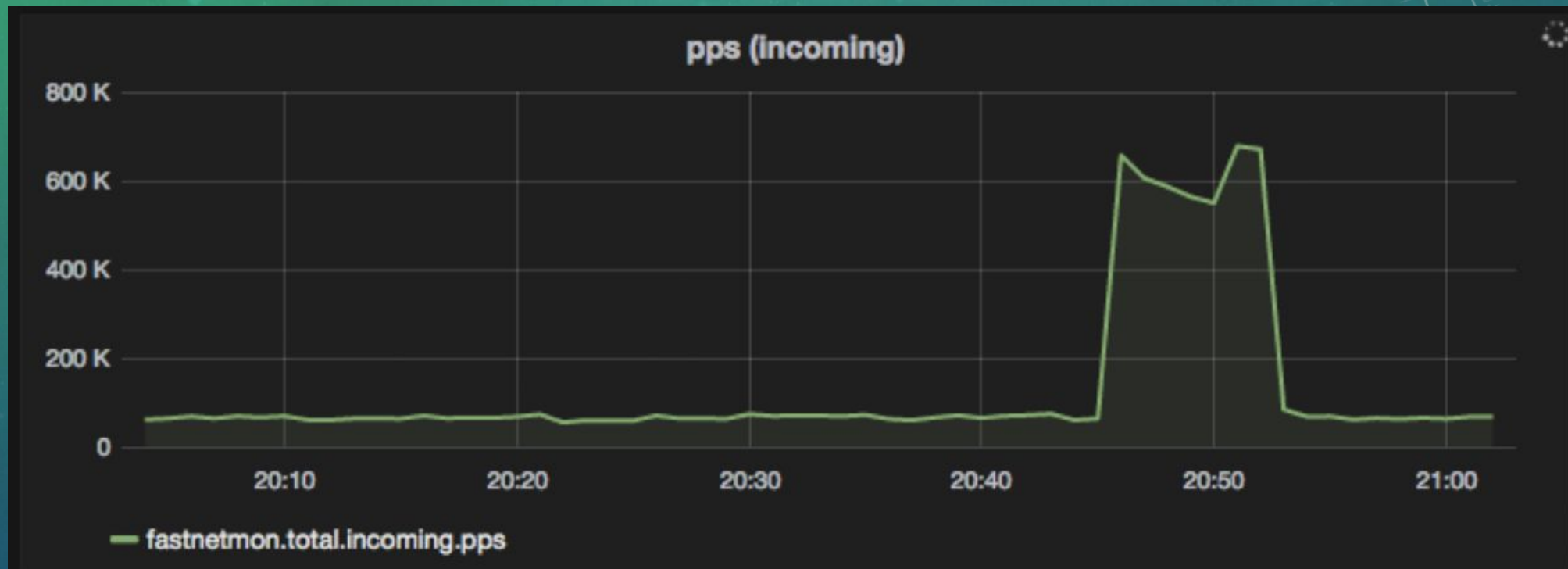


Well, even that one is not a DDoS

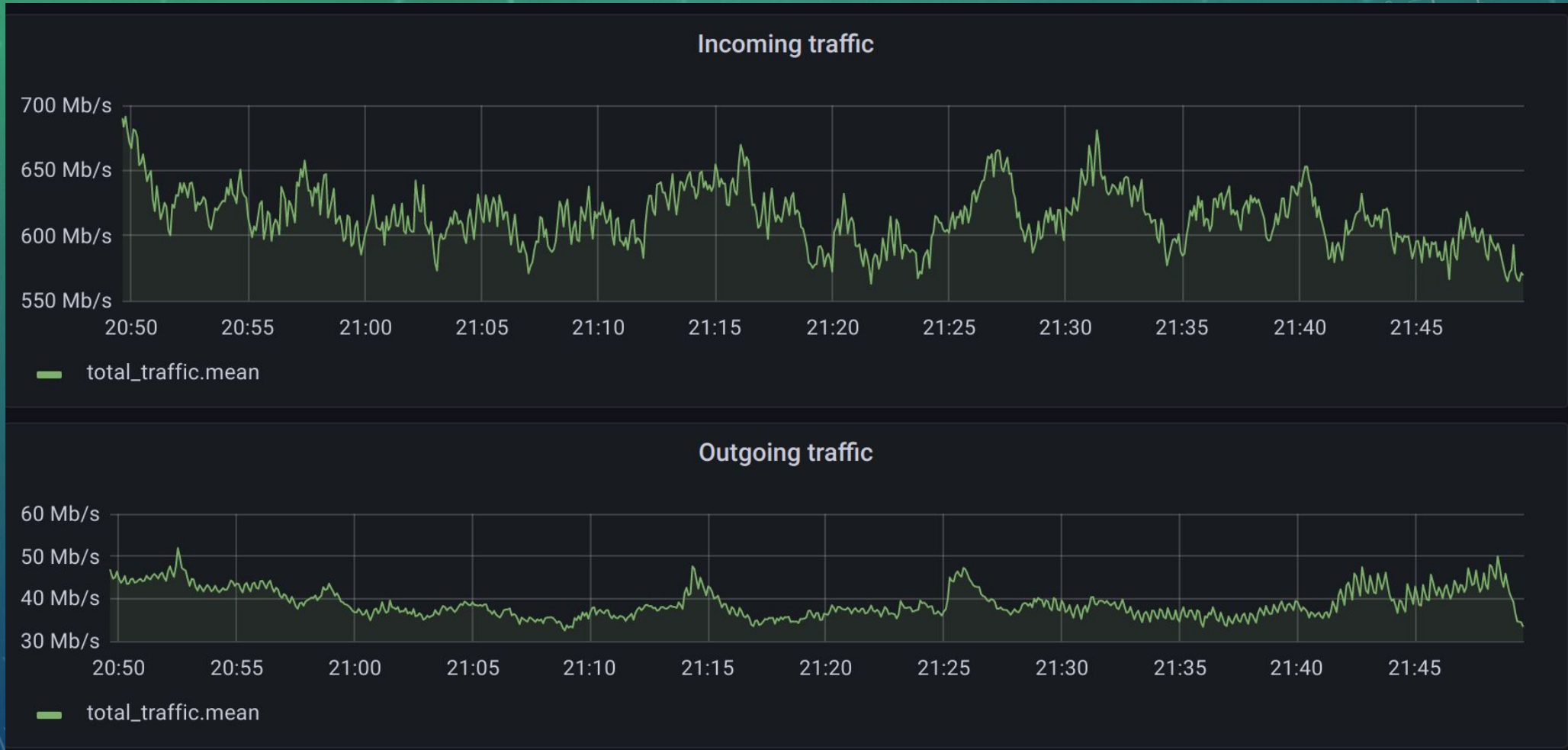




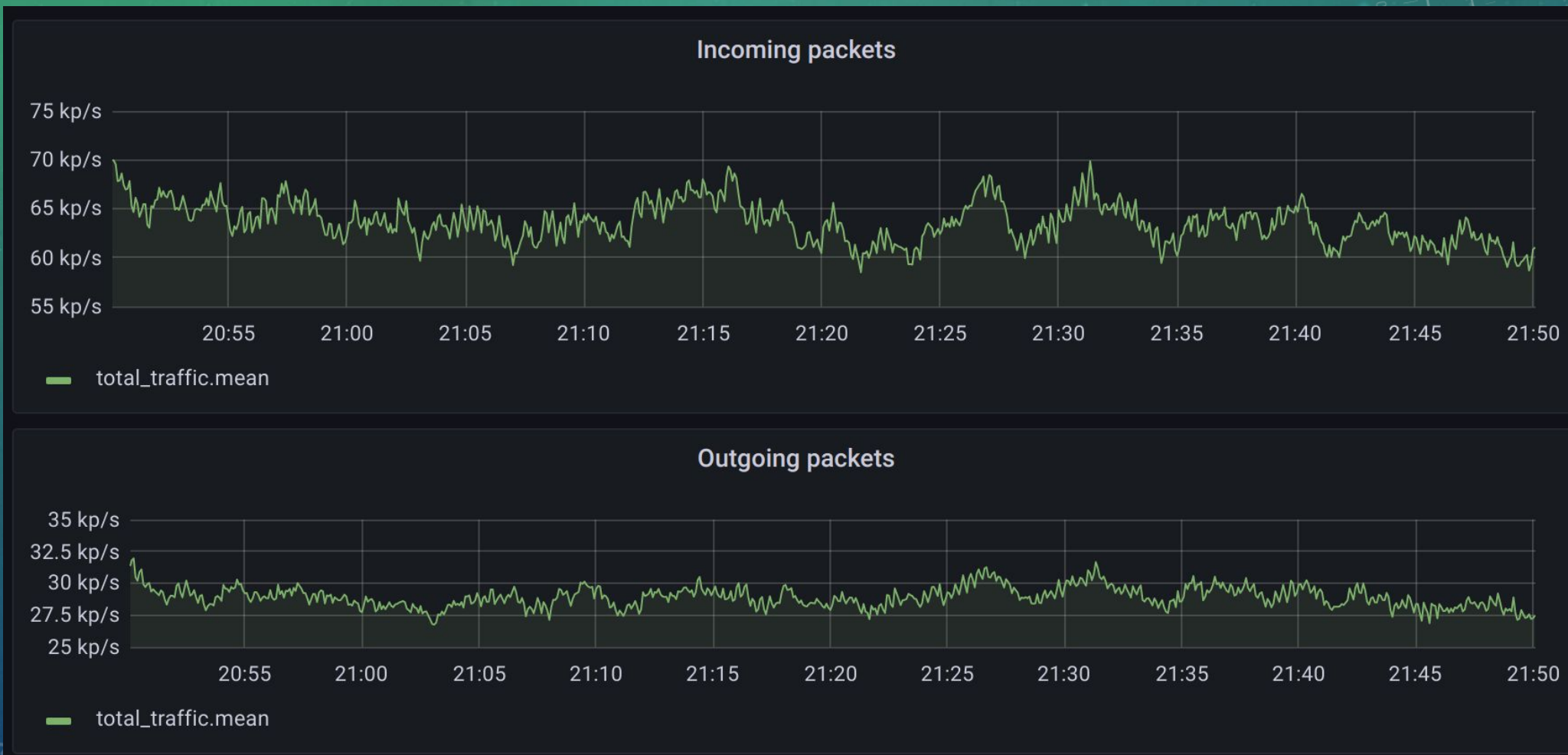
# And that's clearly a DDoS



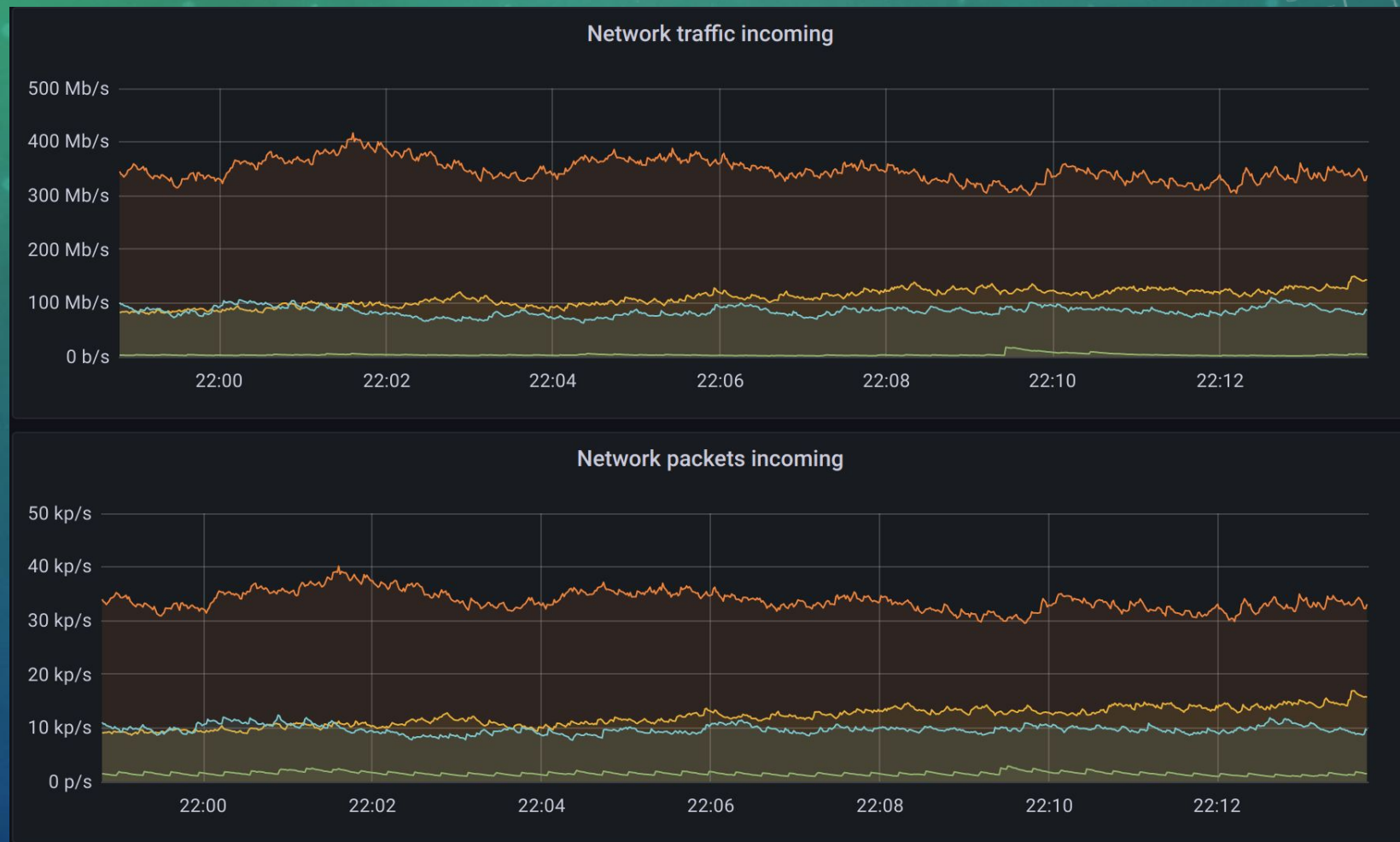
# Total incoming traffic



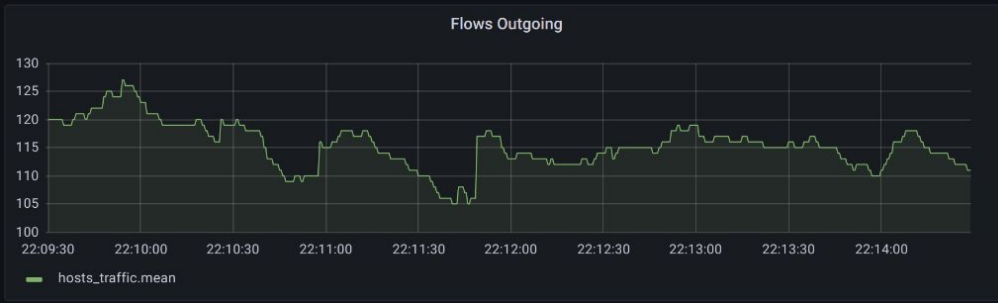
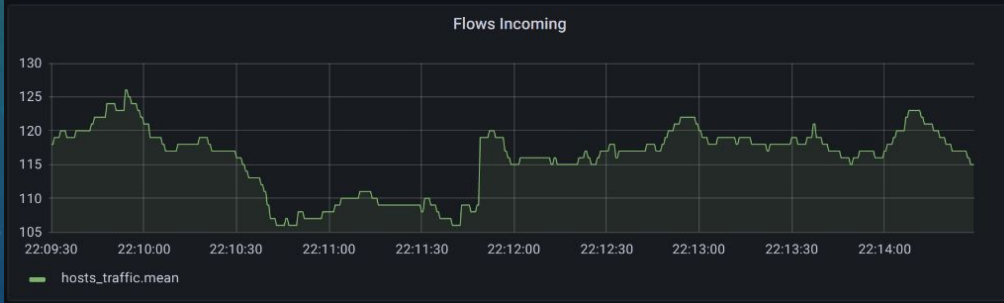
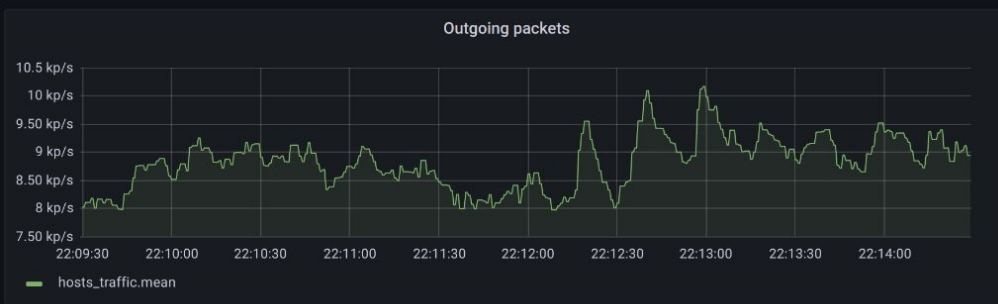
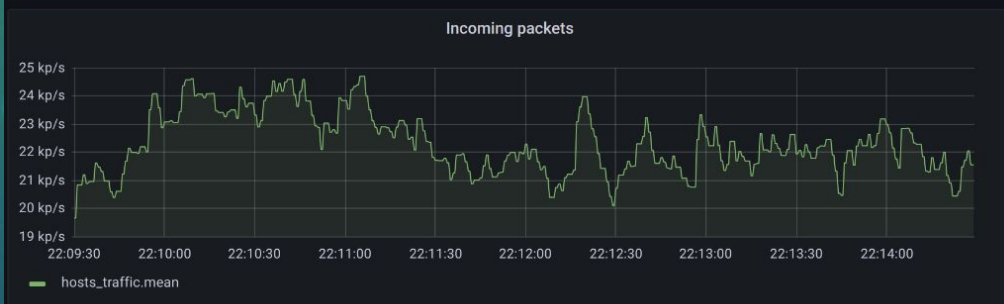
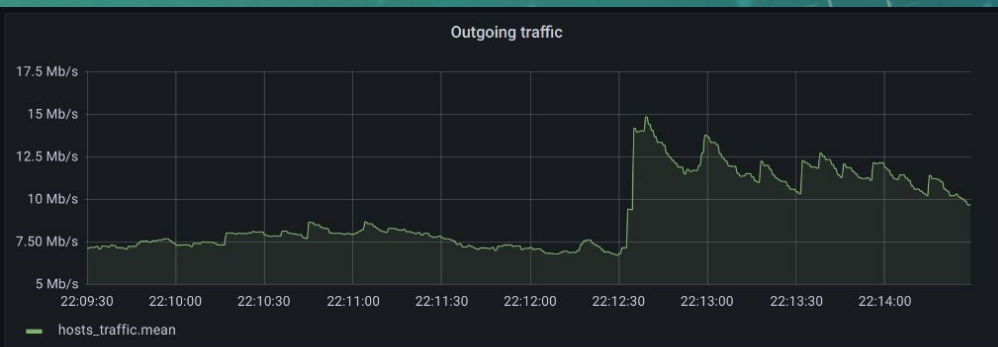
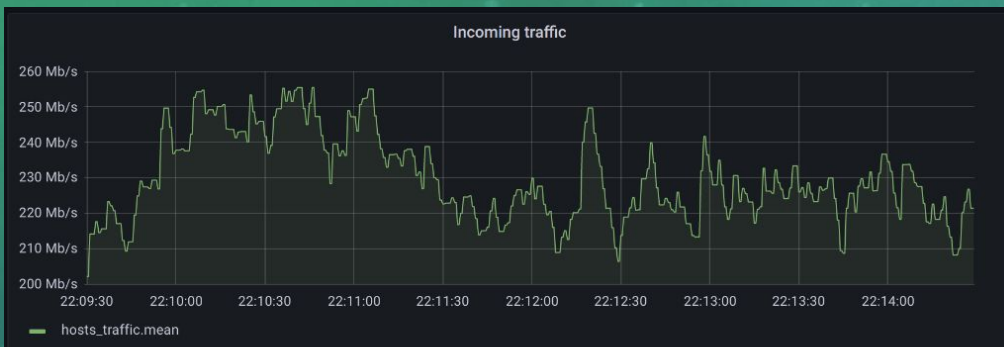
# Total outgoing traffic



# Per network traffic



# Per host traffic



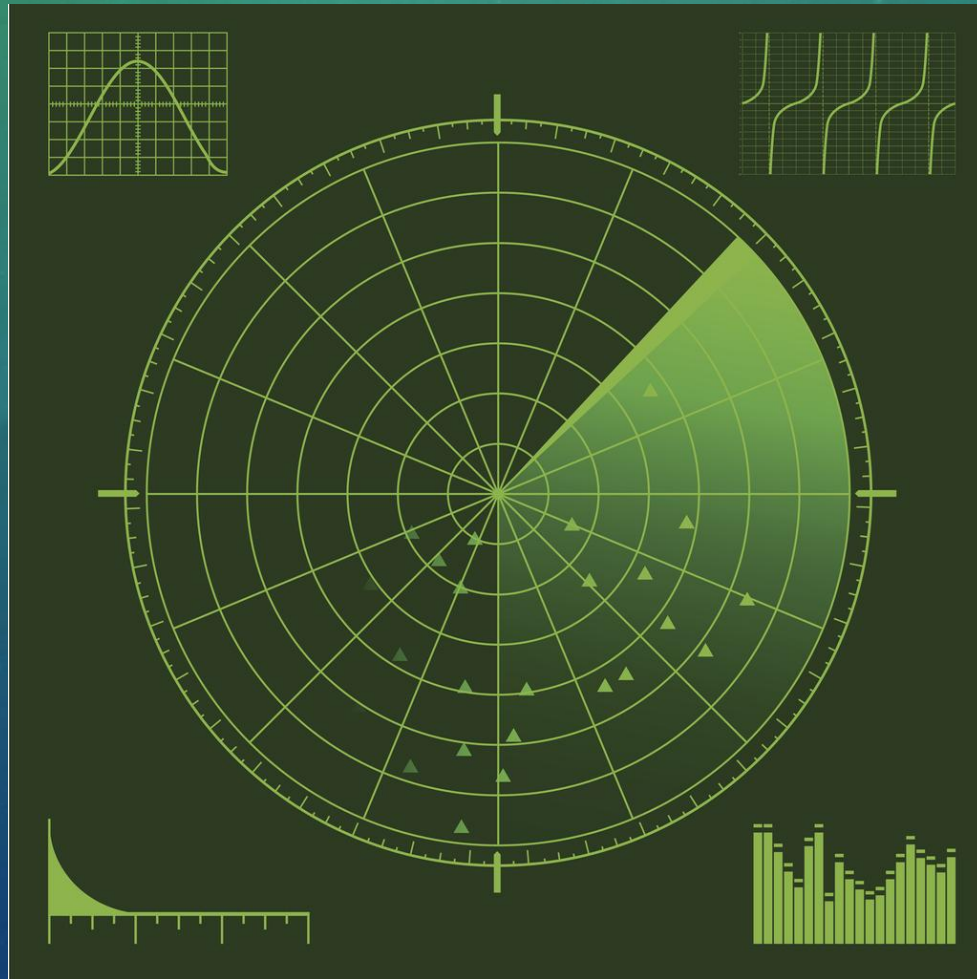
# FastNetMon graphing capabilities

- InfluxDB v1 support
- Graphite support
- Grafana support: dozens of official and community contributed dashboards

# Traffic Capture Backends

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

# What is the target of a DDoS?





# Telco networks are huge



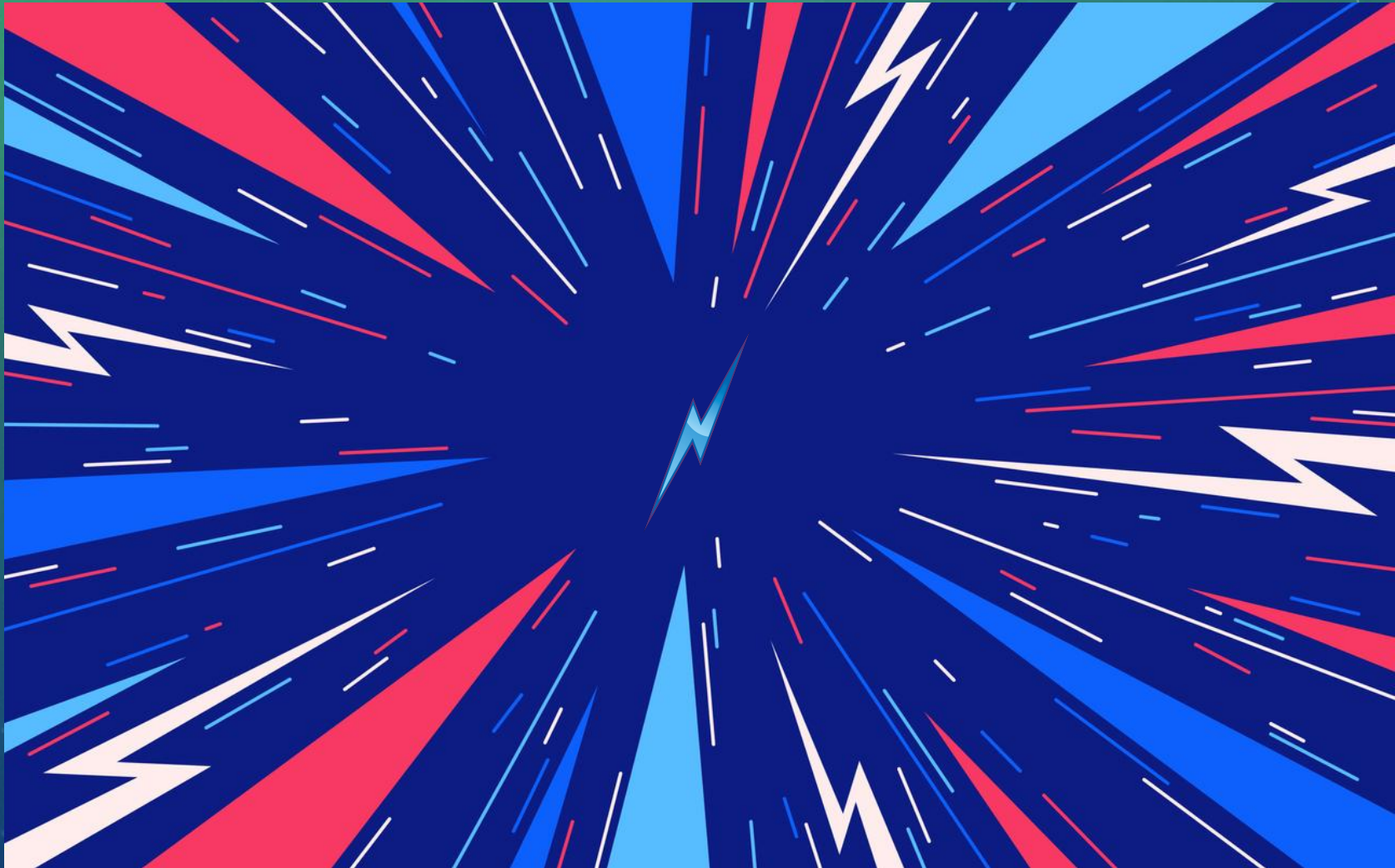
# Data Center networks are complex



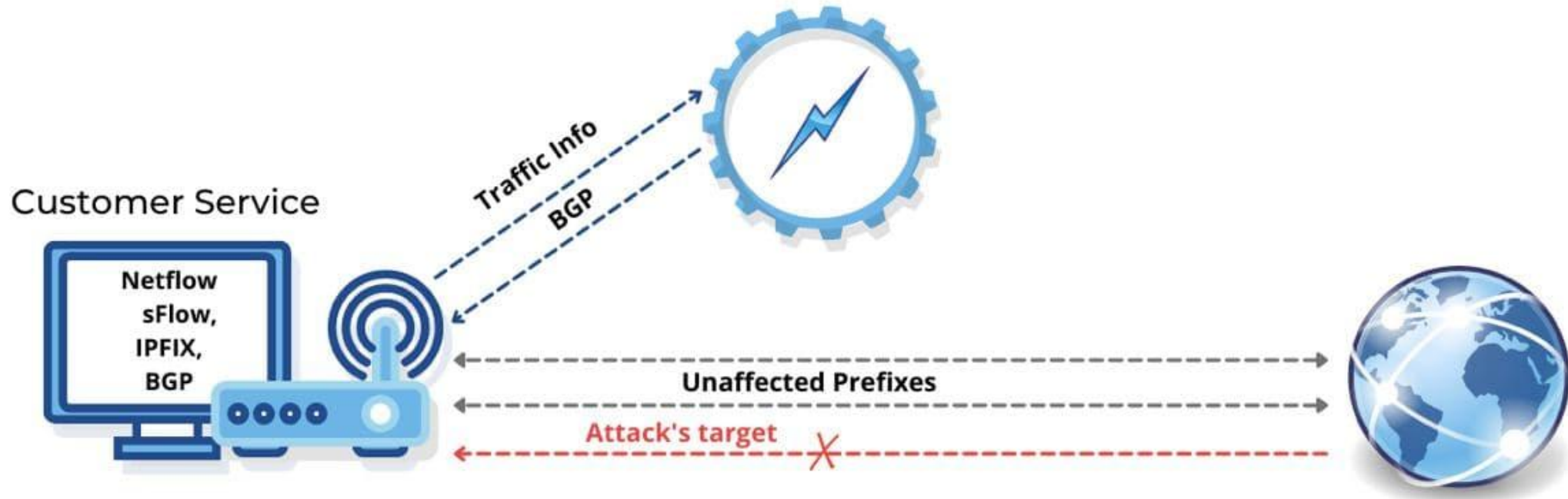
# Thresholds based detection logic

- Mbit per second
- Packet per second
- Flows per second

# FastNetMon detects attacks in seconds



# BGP Blackhole / RTBH support via GoBGP



# 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>

The background is a blue gradient with faint technical diagrams and circular patterns. On the right side, there is a large circular diagram with concentric circles and radial lines, resembling a gauge or a scale. The numbers 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, and 200 are visible along the outer edge of this diagram. There are also smaller circular diagrams and dashed lines scattered across the background.

Thank you!