Lightning Fast DDoS detection

Using FastNetMon Community, part 1

Pavel Odintsov

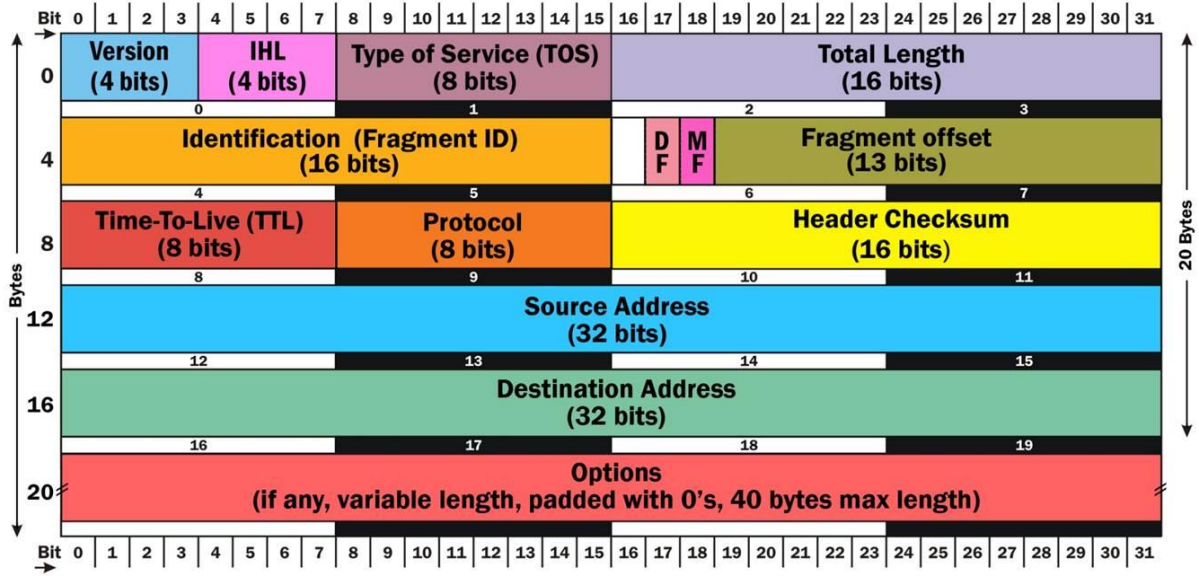
Hello!

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

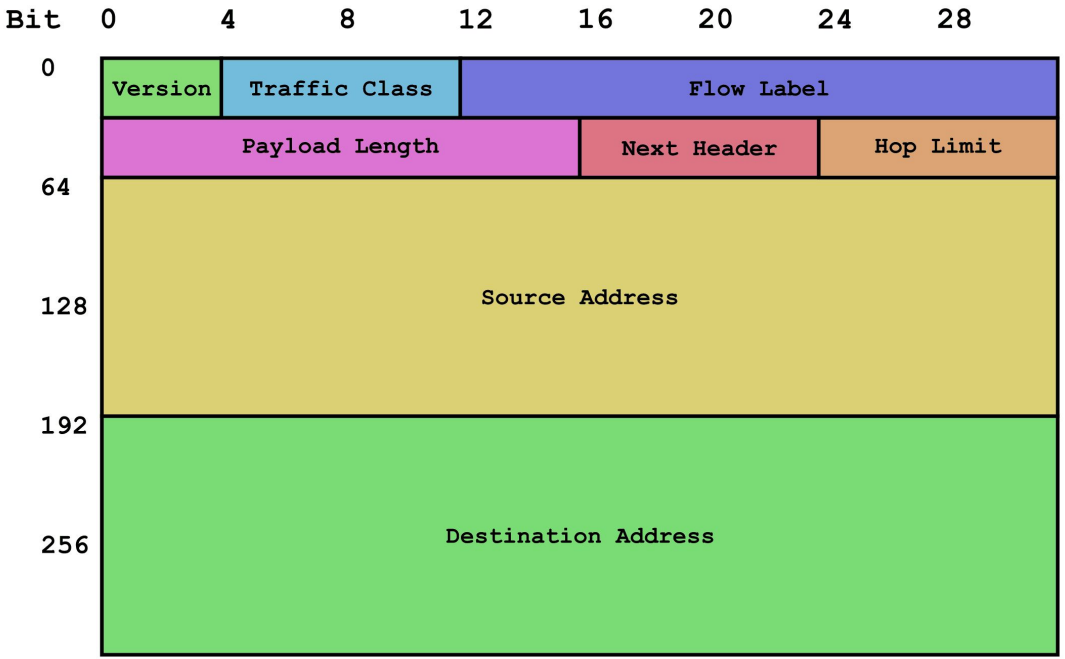
Ways to contact me:

- linkedin.com/in/podintsov
- github.com/pavel-odintsov
- twitter.com/odintsov_pavel
- IRC, FreeNode, pavel_odintsov
- pavel.odintsov@gmail.com

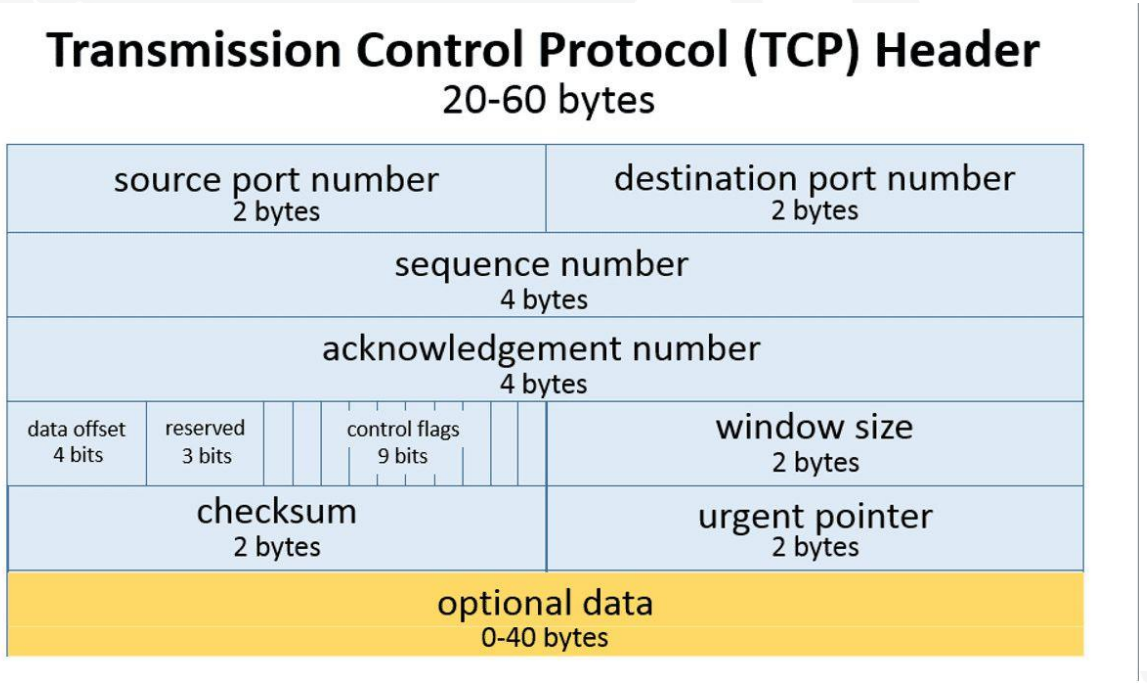
What Kind of DDoS? L3. IPv4



What Kind of DDoS? L3. IPv6



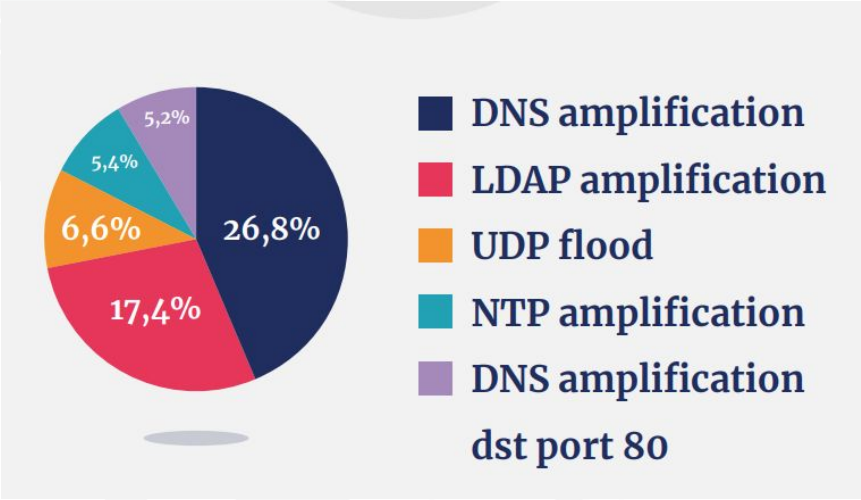
What Kind of DDoS? L4. TCP



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) v1.2

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
- 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)

Supported Vendors

FastNetMon Users

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

Confirmed Scalability

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

* Per physical server

Attack Detection Actions

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

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

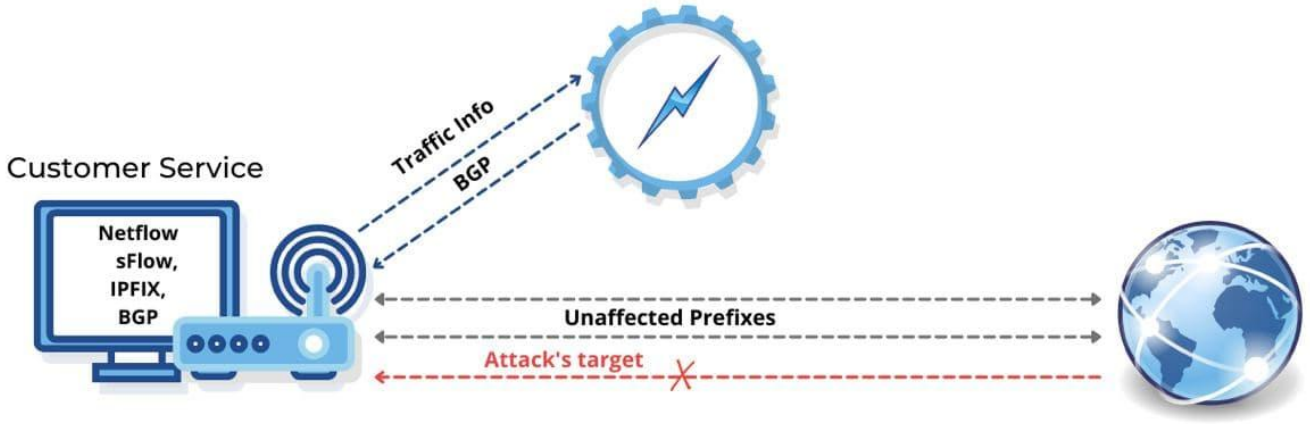
Available Thresholds

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

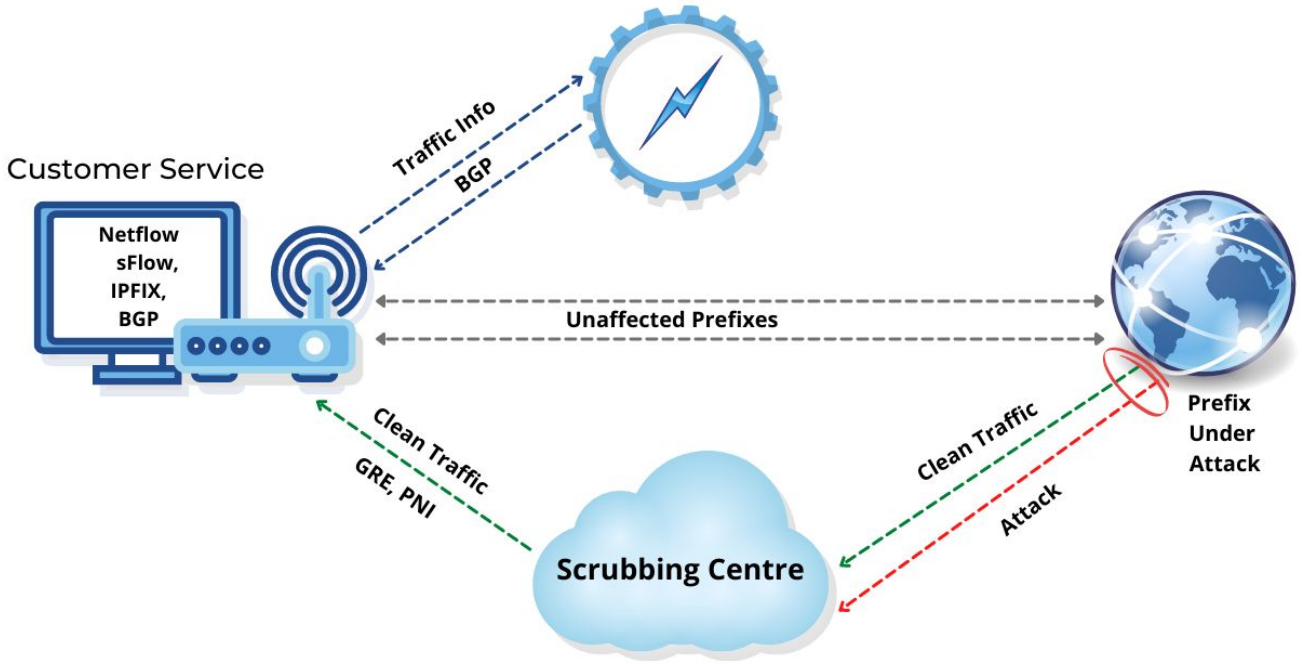
Between Cloud and On Premise

- 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

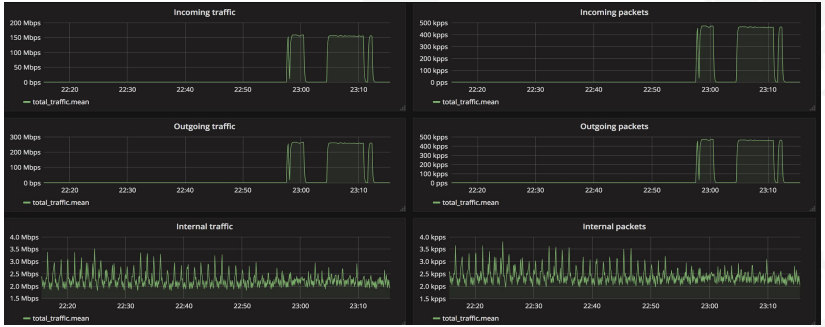
RTBH Automation



Cloud Scrubbing Diversion



Visual Traffic Metrics



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
```

Community

- Site: https://fastnetmon.com/guides/
- GitHub: https://github.com/pavel-odintsov/fastnetmon
- IRC: #fastnetmon at Libera 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/JjwF855pwZvIlasTUsZ7EO
- Mail list: https://groups.google.com/forum/#!forum/fastnetmon

Want to talk?

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

QUESTIONS?

Thank You!