KEY FEATURES

• Supports all types of volumetric attacks
• Completely open source licensed under GPLv2 license
• 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
• Ubuntu 16.04, 18.04, 20.04, 22.04
• RHEL 6, 7, 8, 9
• AlmaLinux, Rocky Linux 8, 9
• CentOS 6, 7, 8
• FreeBSD 9, 10, 11 (ports)
• Cumulus Linux
• VyOS (bundled)
SUPPORTED VENDORS

Arista
Nokia
Juniper Networks
Huawei
A-10 Networks
HP
 Extreme Networks
Dell
Cisco
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 (routers)
- SPAN/MIRROR (1GE, 10GE, 40GE)
SUPPORTED ATTACK TYPES

• NTP, DNS, SNMP, SSDP amplification
• TCP SYN/ACK/SYN-ACK floods
• UDP floods
• Reflection attacks
UNLIMITED SCALABILITY

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

*all numbers for single physical server
ACTIONS TRIGGERED FOR DETECTED ATTACK

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

• Works on any VM or physical server
• Less than 15 minutes to install and configure FastNetMon on new server!
• Learn almost all configuration automatically!
DETECTION LOGIC

Detection type:
• Threshold based (based on host’s average traffic)

THRESHOLD TYPES:
• USING TOTAL TRAFFIC
• USING TOTAL PPS RATE
• PER PROTOCOL
BETWEEN THE CLOUD AND NETWORK EQUIPMENT

- You could use FastNetMon together with precise filtering hardware (A-10 Networks, Radware, Palo-Alto Networks)
- You could use FastNetMon with your favourite DDoS filtering cloud (Voxility, NBIP NaWas, Path.Net, F5)
- You could use FastNetMon to isolate attacked customer in special network using BGP diversion
BGP scrubbing centre diversion
ATTACK AND TRAFFIC VISUALIZATION
RICH ATTACK REPORTS

IP: 10.10.10.221
Attack 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
GoBGP configuration

[global.config]
as = 65001
router-id = "10.166.0.15"
port = 179

[[neighbors]]
[neighbors.config]
neighbor-address = "35.217.26.38"
peer-as = 65001
[neighbors.ebgp-multihop.config]
enabled = true

[[neighbors.afi-safis]]
[neighbors.afi-safis.config]
afi-safi-name = "ipv4-unicast"

[[neighbors.afi-safis]]
[neighbors.afi-safis.config]
afi-safi-name = "ipv6-unicast"

[neighbors.transport.config]
local-address = "10.166.0.15"

gobgp = on
gobgp_next_hop = 0.0.0.0
gobgp_announce_host = on
gobgp_community_host = 65001:666
Default thresholds

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
Community

• Site: https://fastnetmon.com/guides/
• GitHub: https://github.com/pavel-odintsov/fastnetmon
• IRC: #fastnetmon at Libra 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!