



FAST  ***ETMON***

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 ARCHITECTURES

- x86/32
- amd64 / x86_64
- ARM/ARM64
- PowerPC
- PowerPC 64
- Sparc64
- MIPS
- Alpha

SUPPORTED VENDORS

ARISTA NOKIA



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 then 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)

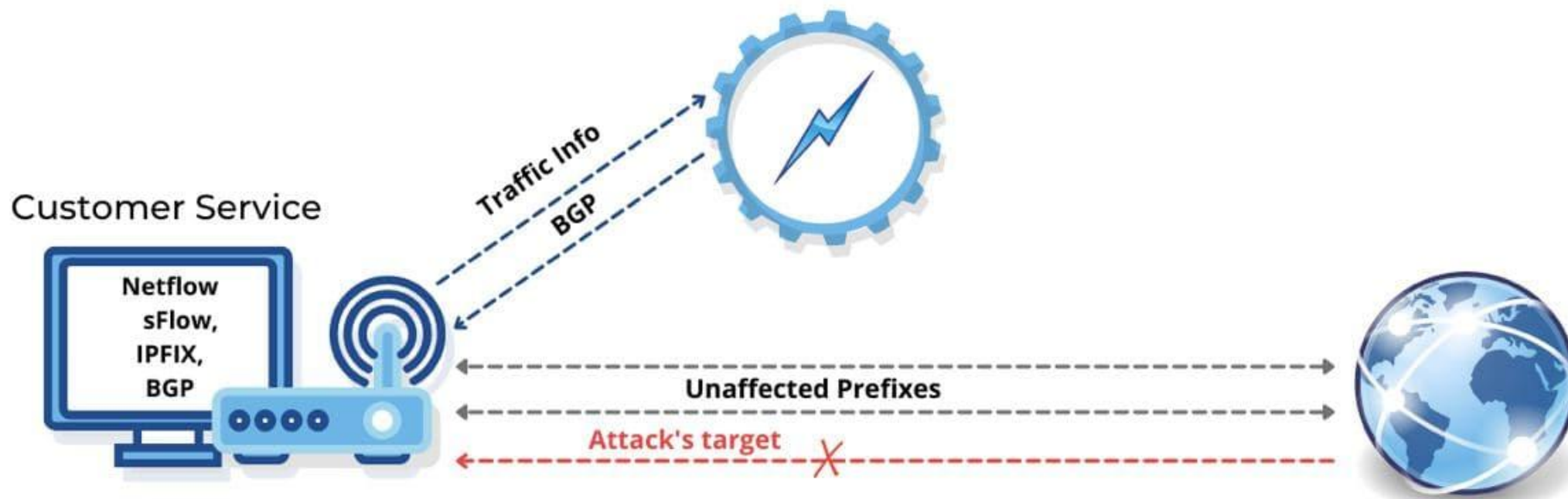
THRESHOLD TYPES:

- USING TOTAL TRAFFIC
- USING TOTAL PPS RATE
- PER PROTOCOL

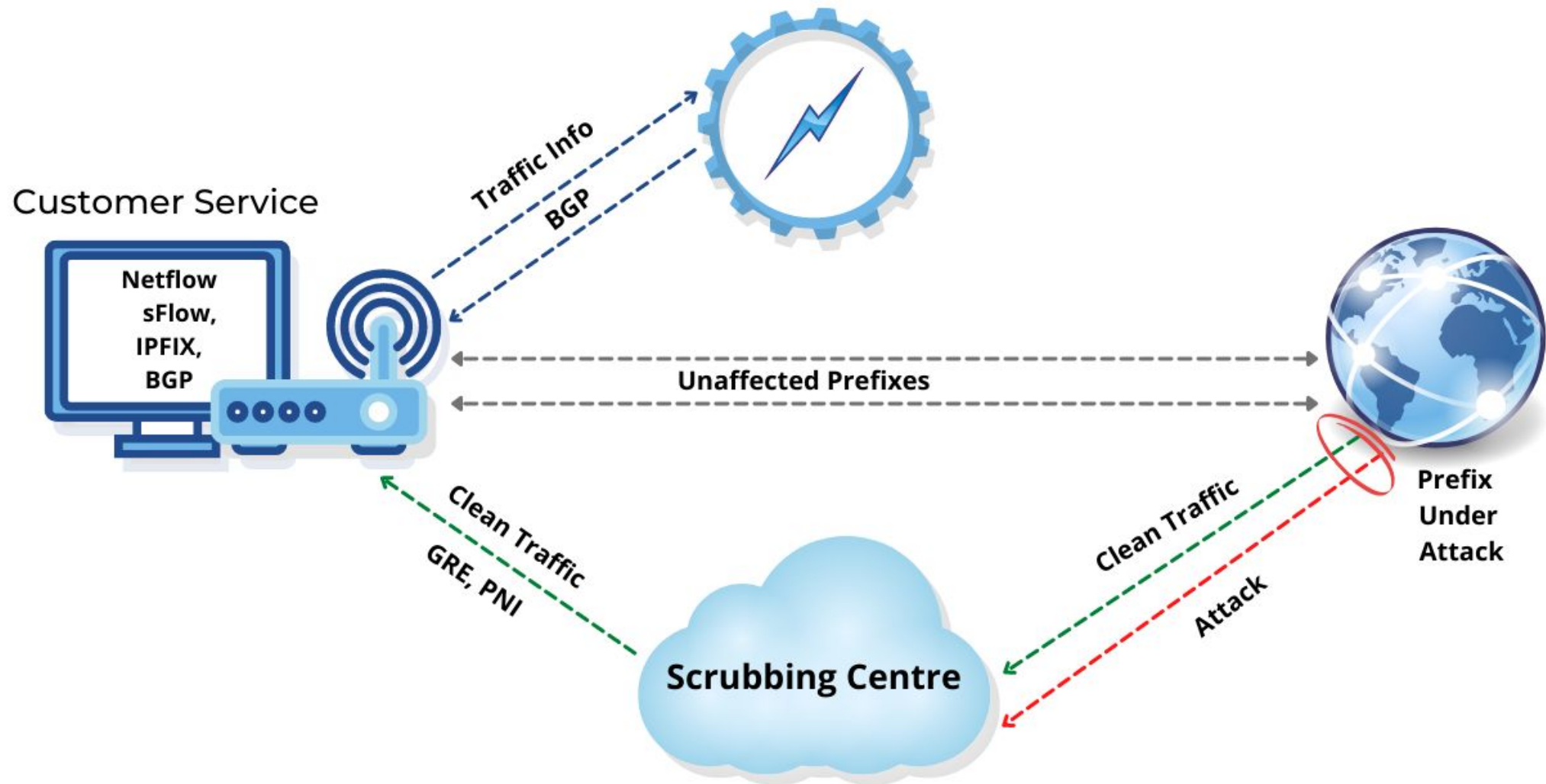
BETWEEN THE CLOUD AND NETWORK EQUIPMENT

- 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
- You could use FastNetMon to isolate attacked customer in special network using BGP diversion

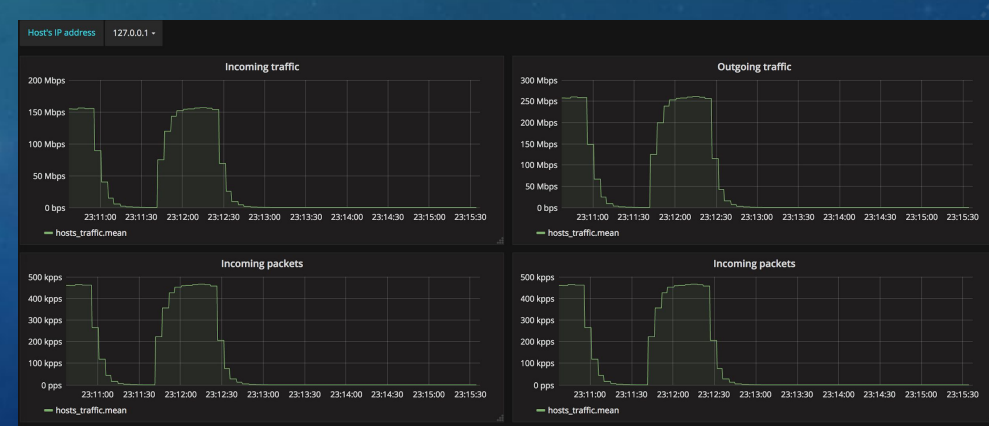
BGP Blackhole / RTBH



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
```

Whole configuration

```
logging:local_syslog_logging = off
logging:remote_syslog_logging = off
logging:remote_syslog_server = 10.10.10.10
logging:remote_syslog_port = 514
enable_ban = on
process_incoming_traffic = on
process_outgoing_traffic = on
ban_details_records_count = 500
ban_time = 1900
unban_only_if_attack_finished = on
enable_subnet_counters = off
networks_list_path = /etc/networks_list
white_list_path = /etc/networks_whitelist
check_period = 1
enable_connection_tracking = off
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
mirror = off
pfring_sampling_ratio = 1
mirror_netmap = off
mirror_snabbswitch = off
mirror_afpacket = off
interfaces_snabbswitch = mac
netmap_sampling_ratio = 1
netmap_read_packet_length_from_ip_header = off
pcap = off
netflow = off
sflow = off
enable_pf_ring_zc_mode = off
interfaces = eth3,eth4
average_calculation_time = 5
average_calculation_time_for_subnets = 20
netflow_port = 2055
netflow_host = 0.0.0.0
netflow_sampling_ratio = 1
netflow_divide_counters_on_interval_length = off
sflow_port = 6343
sflow_host = 0.0.0.0
sflow_qinq_process = off
sflow_qinq_ethertype = 0x8100
notify_script_path = /usr/local/bin/notify_about_attack.sh
notify_script_pass_details = on
collect_attack_pcap_dumps = off
process_pcap_attack_dumps_with_dpi = off
redis_enabled = off
redis_port = 6379
redis_host = 127.0.0.1
redis_prefix = mydc1
```

```
mongodb_enabled = off
mongodb_host = localhost
mongodb_port = 27017
mongodb_database_name = fastnetmon
pfring_hardware_filters_enabled = off
exabgp = off
exabgp_command_pipe = /var/run/exabgp.cmd
exabgp_community = 65001:666
exabgp_next_hop = 10.0.3.114
exabgp_announce_host = on
exabgp_announce_whole_subnet = off
exabgp_flow_spec_announces = off
gobgp = off
gobgp_next_hop = 0.0.0.0
gobgp_announce_host = on
gobgp_announce_whole_subnet = off
graphite = off
graphite_host = 127.0.0.1
graphite_port = 2003
graphite_prefix = fastnetmon
monitor_local_ip_addresses = on
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
pid_path = /var/run/fastnetmon.pid
cli_stats_file_path = /tmp/fastnetmon.dat
enable_api = off
sort_parameter = packets
max_ips_in_list = 7
```

FastNetMon installation

```
odintsov@thinkpad:~$ echo "Check that we run on Ubuntu 20.04 LTS"
Check that we run on Ubuntu 20.04 LTS
odintsov@thinkpad:~$ cat /etc/issue
Ubuntu 20.04.2 LTS \n \l

odintsov@thinkpad:~$ echo "Download FastNetMon unified installer"
Download FastNetMon unified installer
odintsov@thinkpad:~$ wget https://install.fastnetmon.com/installer -O installer
--2021-08-04 11:05:33-- https://install.fastnetmon.com/installer
Resolving install.fastnetmon.com (install.fastnetmon.com)... 151.101.86.132
Connecting to install.fastnetmon.com (install.fastnetmon.com)|151.101.86.132|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 20428983 (19M) [application/octet-stream]
Saving to: 'installer'

installer                               100%[=====>] 19.48M  5.42MB/s   in 3.6s

2021-08-04 11:05:37 (5.42 MB/s) - 'installer' saved [20428983/20428983]

odintsov@thinkpad:~$ echo "Set exec bit to run installer tool"
Set exec bit to run installer tool
odintsov@thinkpad:~$ chmod +x installer
odintsov@thinkpad:~$ echo "Run installer, it will detect Linux distribution and download pre-built packages"
Run installer, it will detect Linux distribution and download pre-built packages
odintsov@thinkpad:~$ sudo ./installer -install community edition
11:05:50 Will log all installation process details into file: /tmp/fastnetmon_install_26789.log
11:05:50 Installer build git version is: 570505c26a4bd41b84717121a45ecb1f1463c8a3 build time is: 2021-07-29T15:59:39
11:05:50 Install FastNetMon Community edition

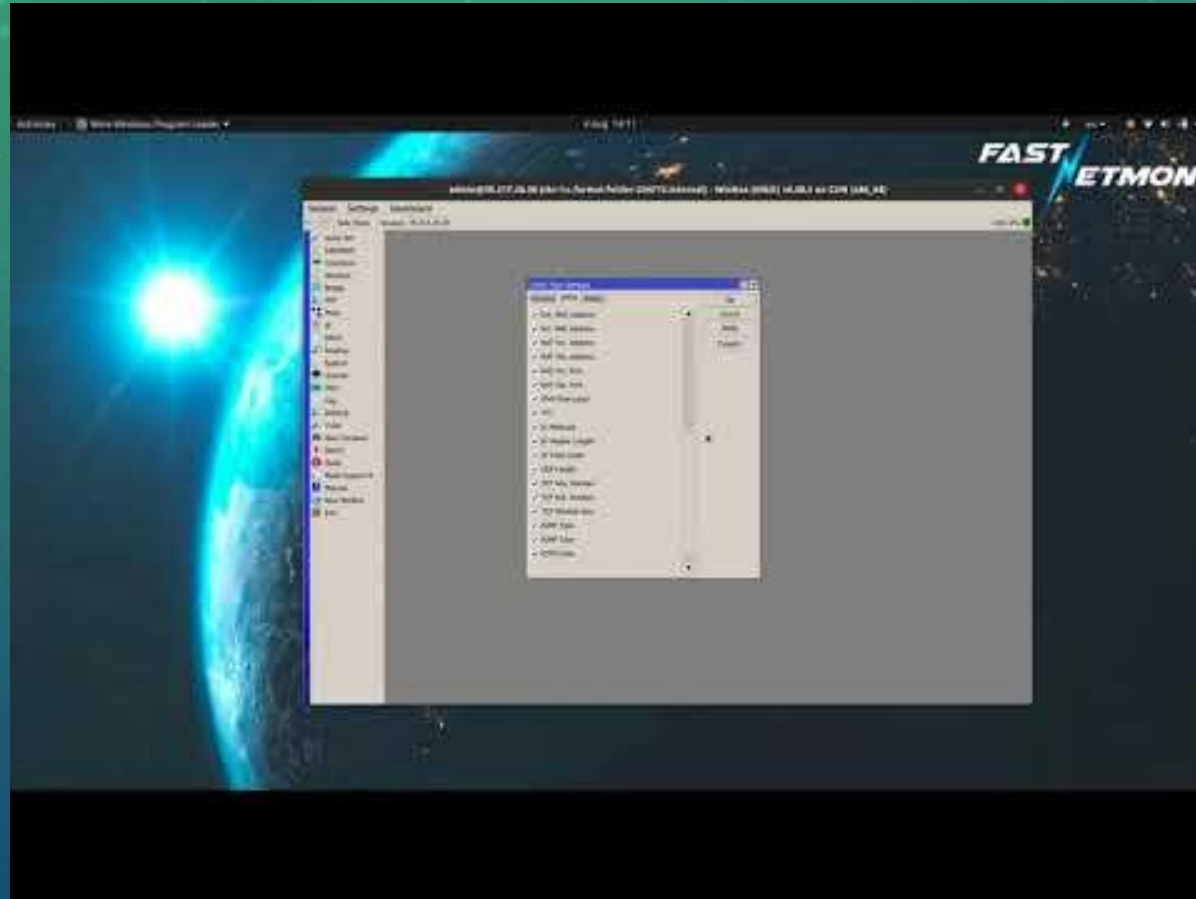
We offer significantly improved FastNetMon Advanced edition: https://fastnetmon.com/fastnetmon-advanced/?utm_source=community_install_script&utm_medium=email
You could order free one-month trial for Advanced edition here: https://fastnetmon.com/trial/?utm_source=community_install_script&utm_medium=email

To use FastNetMon Community you must provide your valid corporate email and accept to receive information about our commercial edition and security updates.
You can find our privacy policy here https://fastnetmon.com/privacy-policy/

Provide your corporate email here, personal emails are not allowed: pavel.odintsov@gmail
```

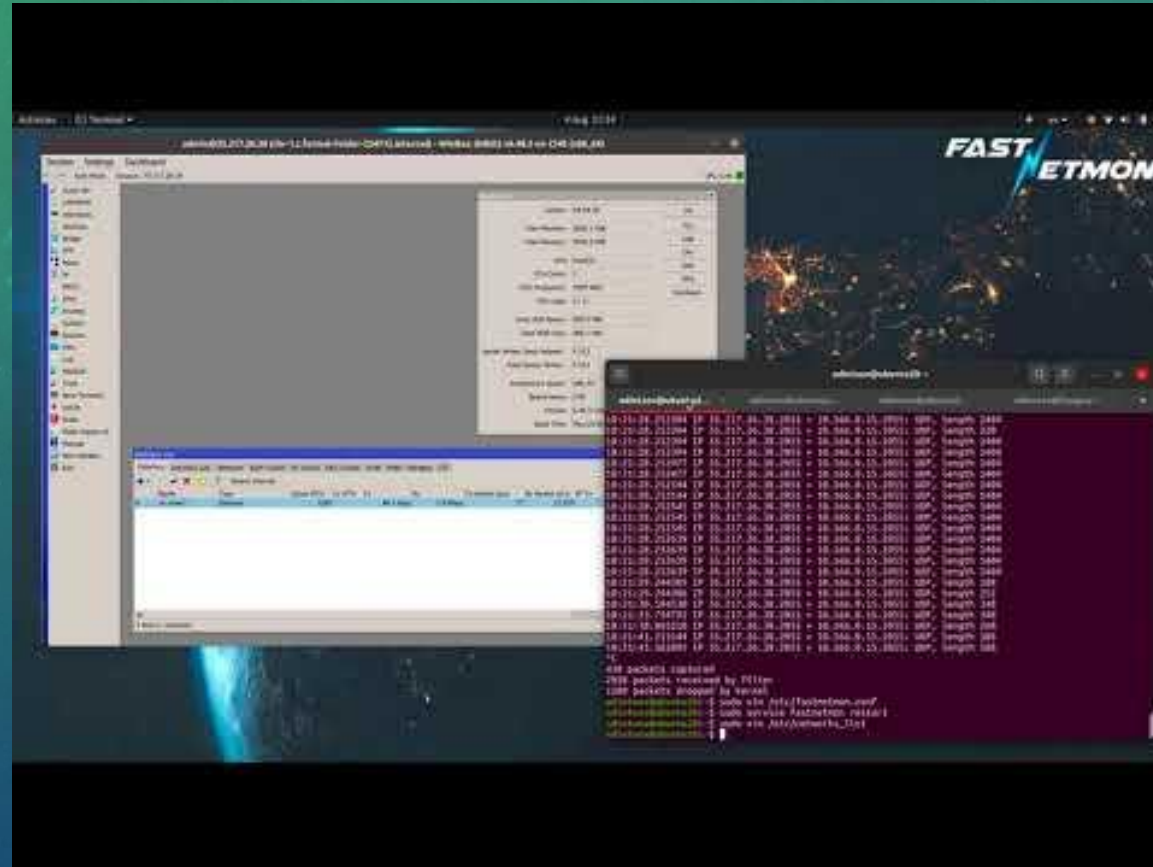
<https://asciinema.org/a/428813>

Mikrotik Netflow setup



<https://www.youtube.com/watch?v=034tFYimU8U>

FastNetMon configuration with Mikrotik Netflow



https://www.youtube.com/watch?v=7r2DUDjD_L8

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
```

FastNetMon and BGP unicast setup

```
# exabgp_community = [65001:666 65001:777]

# specify different communities for host and subnet announces
# exabgp_community_subnet = 65001:667
# exabgp_community_host = 65001:668

exabgp_next_hop = 10.0.3.114

# In complex cases you could have both options enabled and announce host and subnet simultaneously

# Announce /32 host itself with BGP
exabgp_announce_host = on

# Announce origin subnet of IP address instead IP itself
exabgp_announce_whole_subnet = off

# Announce Flow Spec rules when we could detect certain attack type
# Please be aware! Flow Spec announce triggered when we collect some details about attack,
# i.e. when we call attack_details script
# Please disable exabgp_announce_host and exabgp_announce_whole_subnet if you want to use this feature
# Please use ExaBGP v4 only (Git version), for more details: https://github.com/pavel-odintsov/fastnetmon/blob/master/docs/BGP_FLOW_SPEC.md
exabgp_flow_spec_announces = off

# GoBGP intergration
gobgp = on

# Configuration for IPv4 announces
gobgp_next_hop = 0.0.0.0
gobgp_announce_host = on
gobgp_announce_whole_subnet = off

gobgp_community_host = 65001:666
gobgp_community_subnet = 65001:777

# Configuration for IPv6 announces
gobgp_next_hop_ipv6 = 100::1
gobgp_announce_host_ipv6 = off
gobgp_announce_whole_subnet_ipv6 = off

gobgp_community_host_ipv6 = 65001:666
gobgp_community_subnet_ipv6 = 65001:777

# Graphite monitoring
# InfluxDB is also supported, please check our reference:
# https://github.com/pavel-odintsov/fastnetmon/blob/master/docs/INFLUXDB_INTEGRATION.md
graphite = off
# Please use only IP because domain names are not allowed here
graphite_host = 127.0.0.1
graphite_port = 2003
```

<https://asciinema.org/a/428962>

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
```

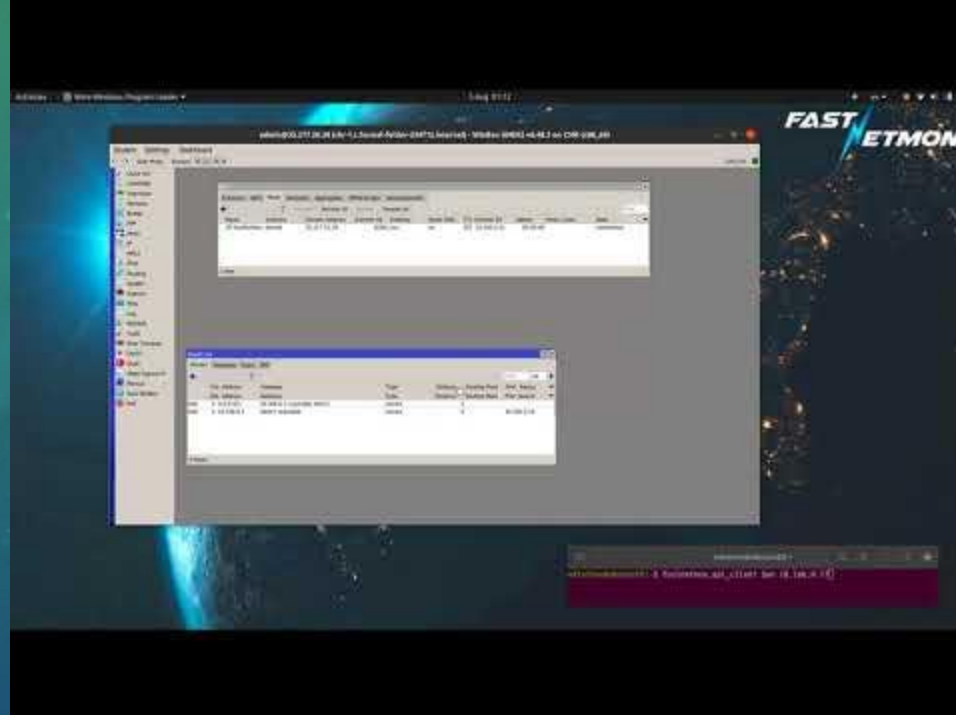
```
hostgroup = my_hosts:10.10.10.221/32,10.10.10.222/32
```

```
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
```

FastNetMon and Mikrotik BGP integration



<https://www.youtube.com/watch?v=JSWaxbwF3w4&t=24s>

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>
- Mail list: <https://groups.google.com/forum/#!forum/fastnetmon>



Thank you!