



# Lightning Fast DDoS detection

Using FastNetMon Community, part 2: installation and setup

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](https://www.linkedin.com/in/podintsov)
- [github.com/pavel-odintsov](https://github.com/pavel-odintsov)
- [twitter.com/odintsov\\_pavel](https://twitter.com/odintsov_pavel)
- IRC, FreeNode, `pavel_odintsov`
- [pavel.odintsov@gmail.com](mailto:pavel.odintsov@gmail.com)

# 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 -Oinstaller
--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

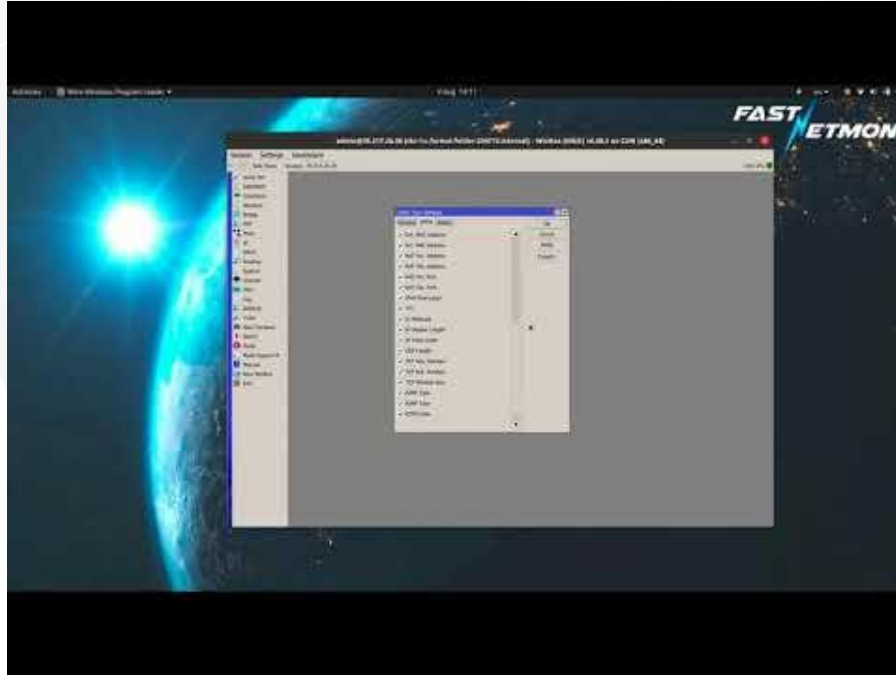
We offer significantly improved FastNetMon Advanced edition: https://fastnetmon.com/fastnetmon-advanced/?utm_source=community_install_script&utm_medium=email
You could order free one-month trial for Advanced edition here: https://fastnetmon.com/trial/?utm_source=community_install_script&utm_medium=email

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
```

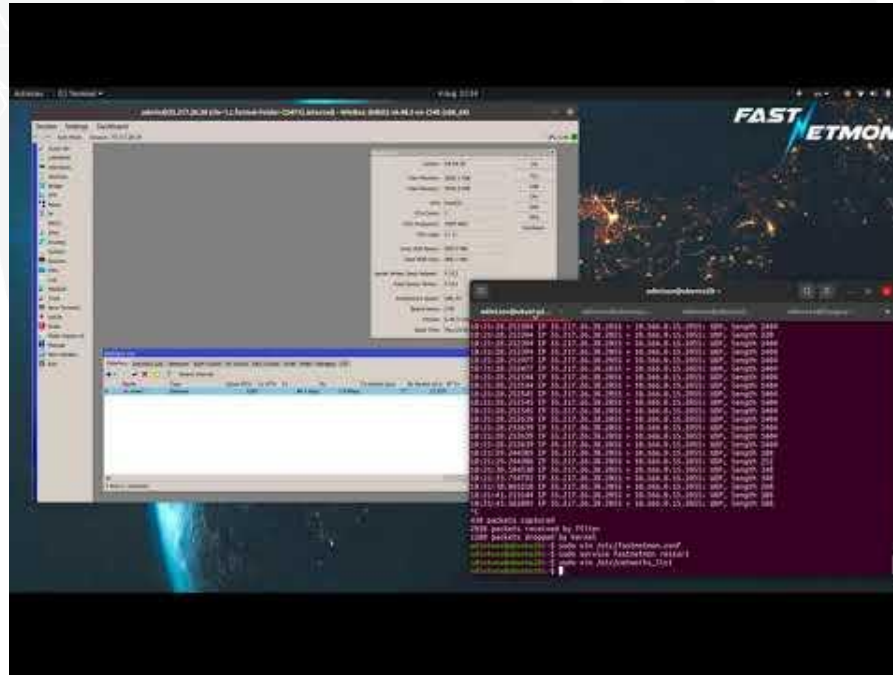
<https://asciinema.org/a/428813>

# Mikrotik Netflow setup



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

# FastNetMon and Mikrotik Netflow



[https://www.youtube.com/watch?v=7r2DUDjD\\_L8](https://www.youtube.com/watch?v=7r2DUDjD_L8)

# GoBGP configuration

```
[global.config]
```

```
as = 65001  
router-id = "10.166.0.15"  
port = 179
```

```
gobgp = on  
gobgp_next_hop = 0.0.0.0  
gobgp_announce_host = on  
gobgp_community_host = 65001:666
```

```
[[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"
```

# FastNetMon and BGP Unicast

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

# specify different communities for host and subnet announces
# exabgp_community_subnet = 65001:667
# exabgp_community_host = 65001:666

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 intergation
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
▶ 00:00
```

<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
```

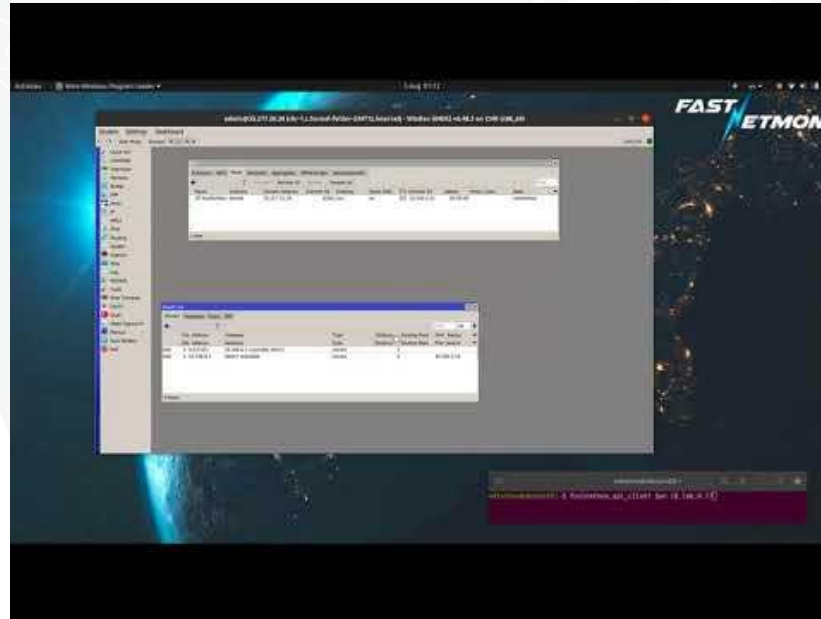
```
my_hosts_enable_ban = off
```

```
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



<https://www.youtube.com/watch?v=JSWaxbwF3w4>

# 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/2o5ldx8>
- LinkedIn: <https://www.linkedin.com/company/fastnetmon/>
- Facebook: <https://www.facebook.com/fastnetmon/>
- WhatsApp: <https://chat.whatsapp.com/JjwF855pwZvllasTUsZ7EO>
- Mail list: <https://groups.google.com/forum/#!forum/fastnetmon>

# Want to talk?

- [linkedin.com/in/podintsov](https://www.linkedin.com/in/podintsov)
- [github.com/pavel-odintsov](https://github.com/pavel-odintsov)
- [twitter.com/odintsov\\_pavel](https://twitter.com/odintsov_pavel)
- IRC, Libera Chat, `pavel_odintsov`
- [pavel@fastnetmon.com](mailto:pavel@fastnetmon.com)



QUESTIONS?

# Thank You!

