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

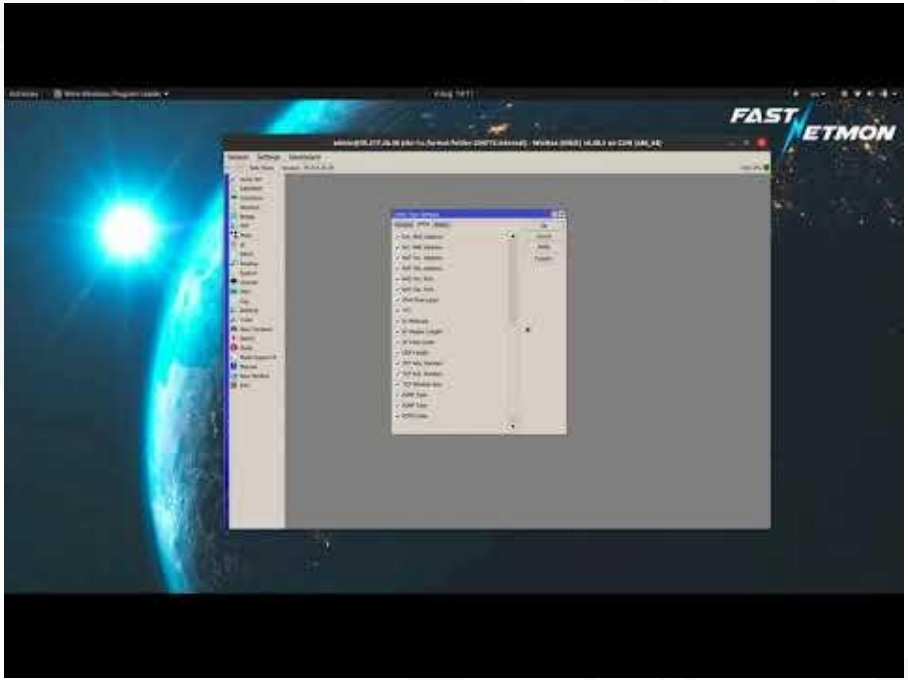
Ways to contact me:

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

FastNetMon installation

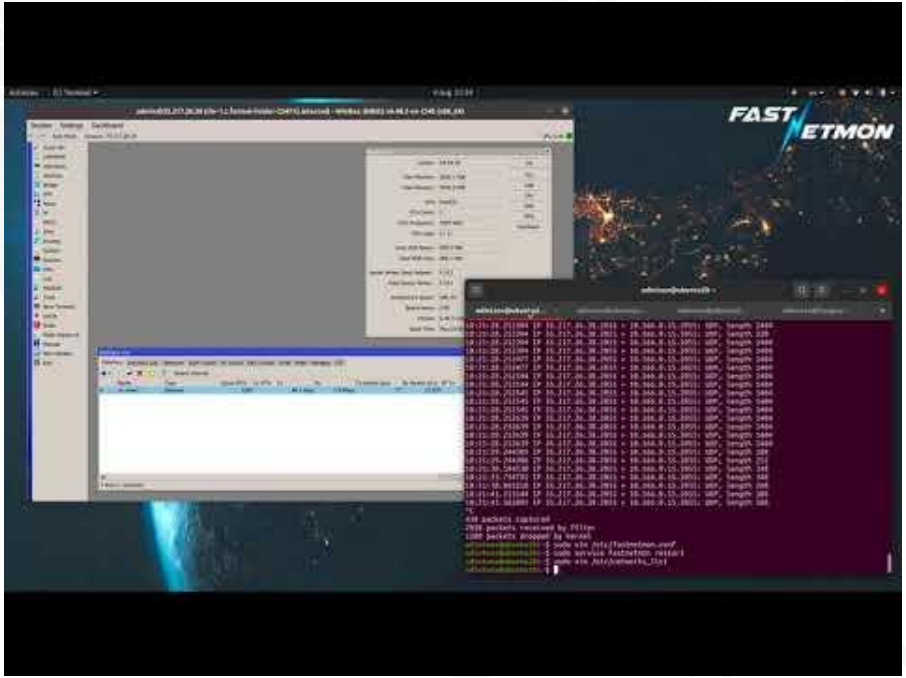
https://asciinema.org/a/428813

Mikrotik Netflow setup



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

FastNetMon and Mikrotik Netflow



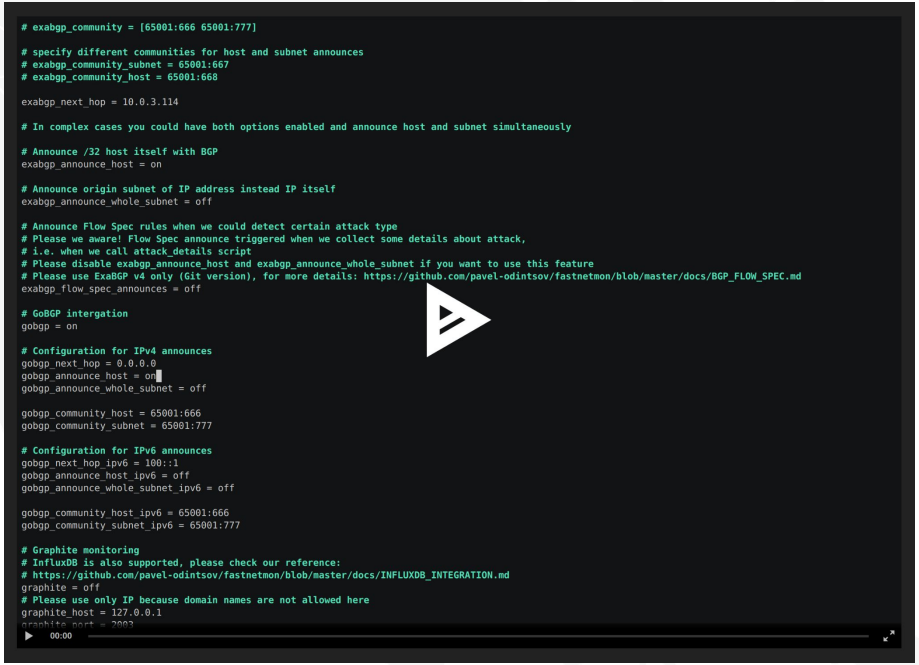
https://www.youtube.com/watch?v=7r2DUDjD_L8

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



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

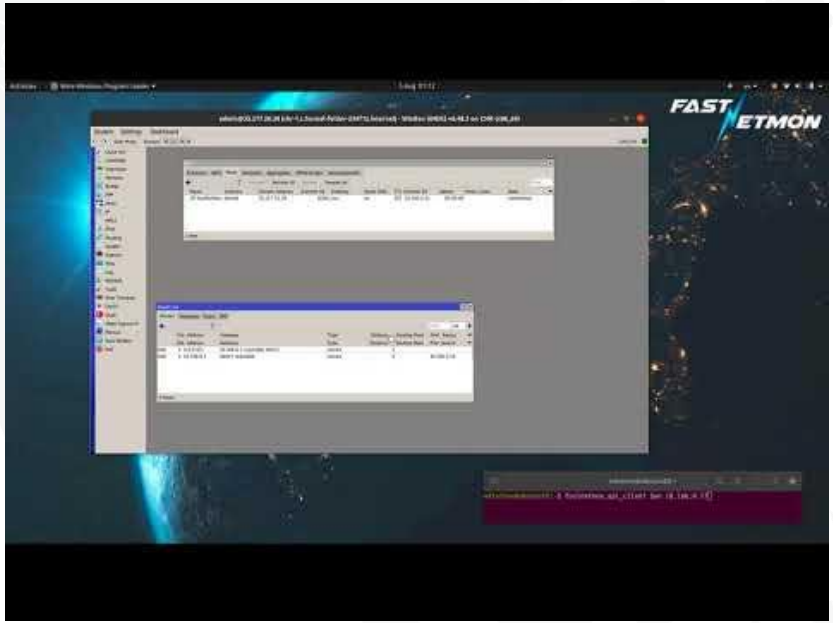
hostgroup =
my_hosts:10.10.10.221/32,10.10.10.222/32

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/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!