
Mikrotik’s
traffic
flow

Hello!

I am Isa Pangestu

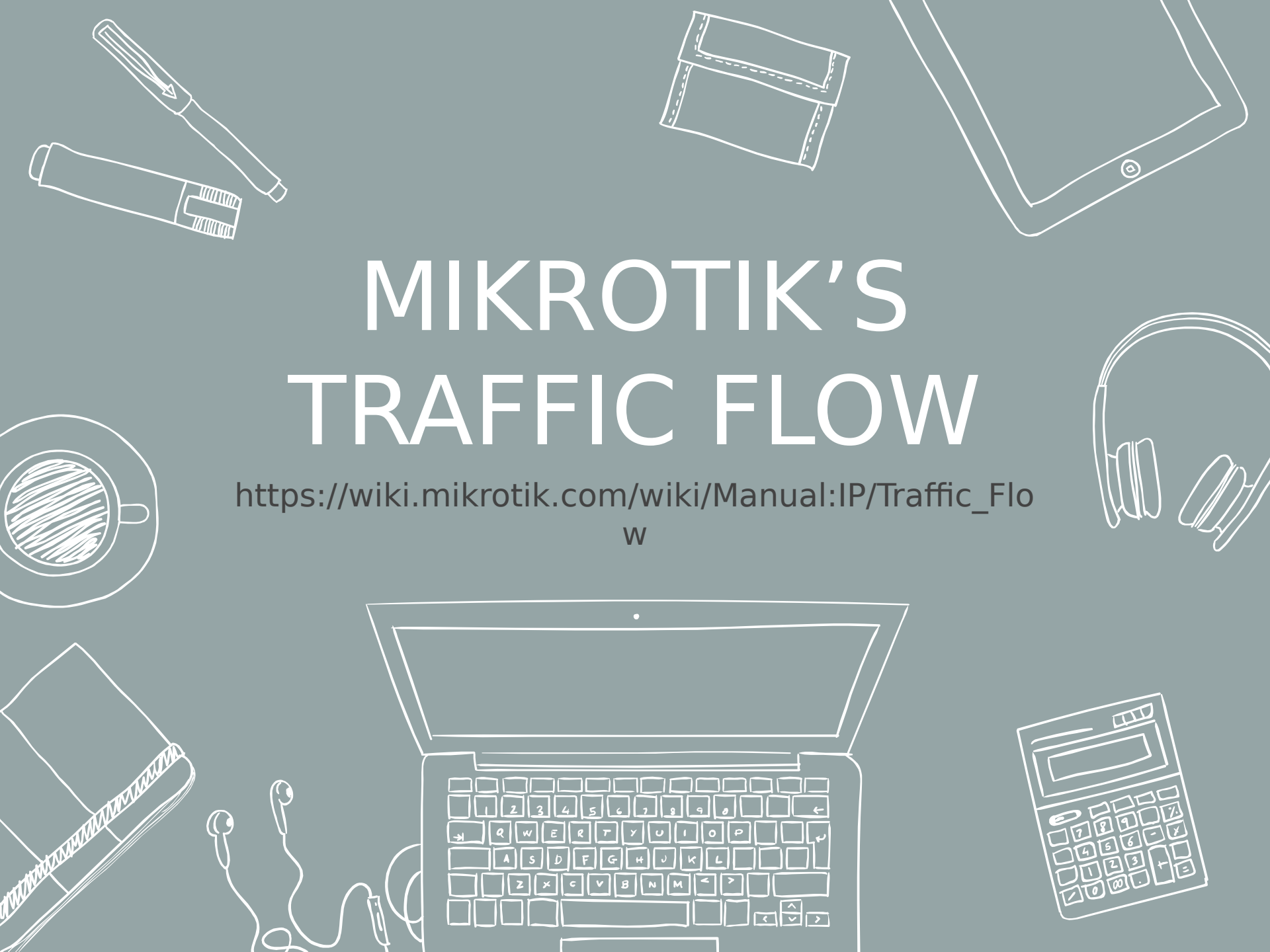
25 yo. Single. NE at PT. Infinys System Indonesia

Used Mikrotik since : 2013
Certificates of Mikrotik : MTCNA, MTCRE, MTCINE

Sharing is Caring. I’d also love to get new experiences and projects ☺

MIKROTIK'S TRAFFIC FLOW

https://wiki.mikrotik.com/wiki/Manual:IP/Traffic_Flow



MikroTik Traffic-Flow is a system that provides statistic information about packets which pass through the router.

Advantage(s)

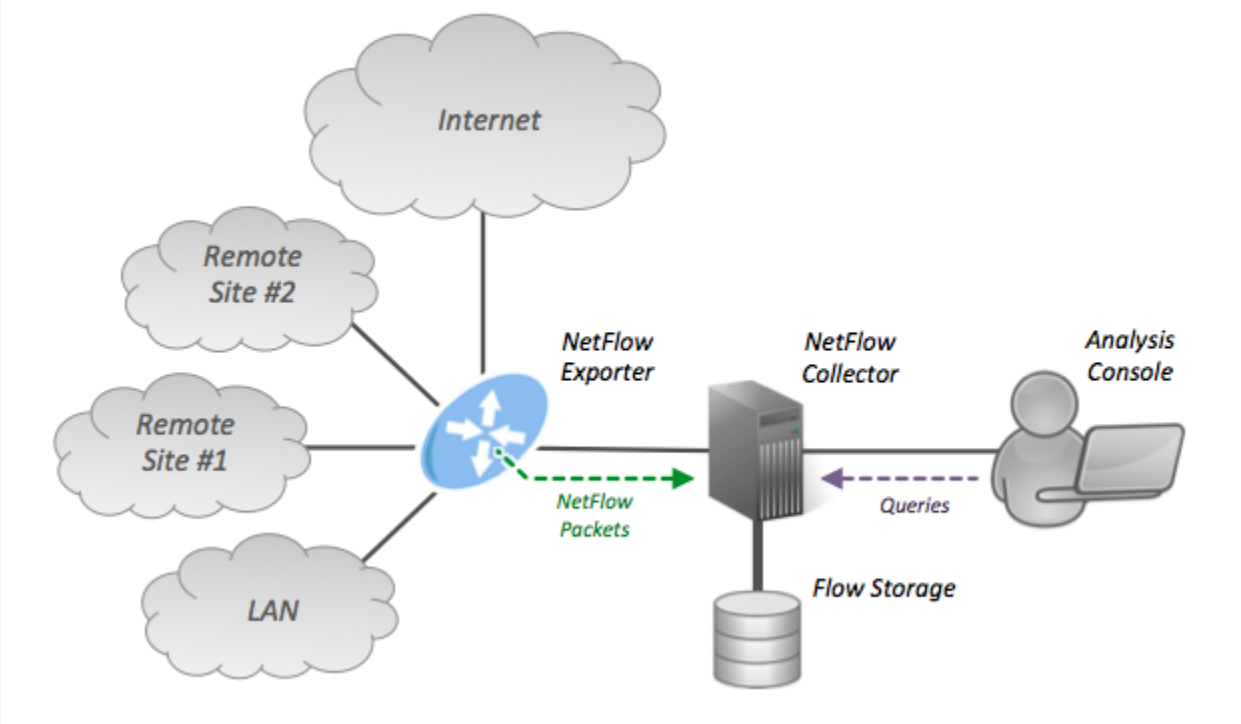
- ✖ Network Monitoring
- ✖ Network Accounting
- ✖ Identify your network

FLOW PROTOCOLS

- ✖ Netflow : Cisco
- ✖ jFlow : Juniper
- ✖ sFlow : Dell, HP
- ✖ Traffic Flow : Mikrotik
- ✖ Netstream : Huawei
- ✖ ...etc

FLOW ROLES

- ✖ Flow Exporter : export flows records towards flow collectors
- ✖ Flow Collector : processing of flow data received from a flow exporter
- ✖ Analysis Apps : analyzed received flow data



Flow Architecture
https://en.wikipedia.org/wiki/NetFlow#/media/File:NetFlow_Architecture_2012.png

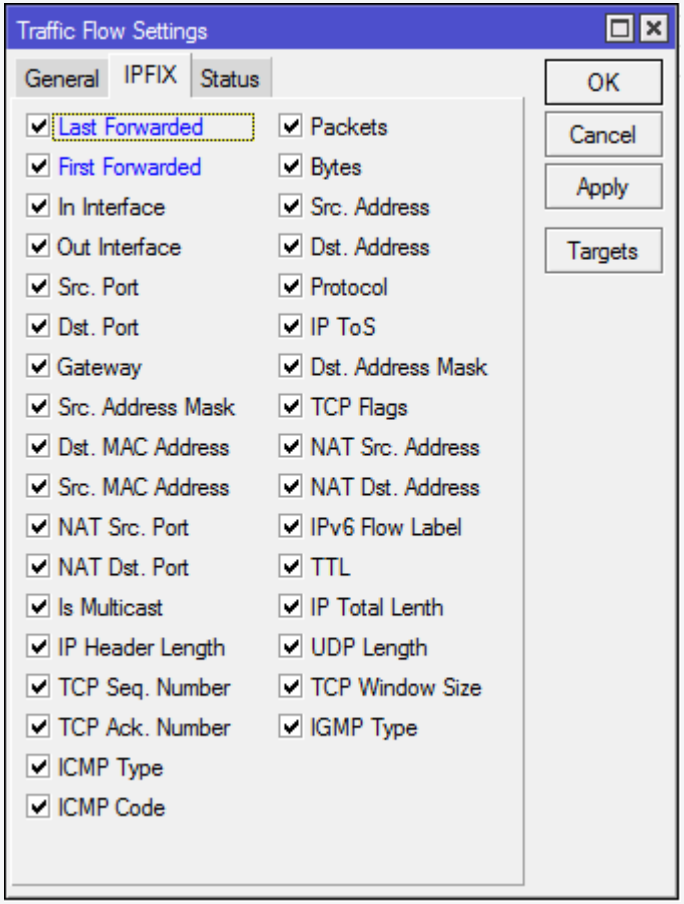
TRAFFIC FLOW FORMATS :

- **version 1** - the first version of NetFlow data format, do not use it, unless you have to

- **version 5 - V**ersion 5 has possibility to include BGP AS and flow sequence number information. Currently RouterOS does not include BGP AS numbers.

- **version 9** - a new format which can be extended with new fields and record types thank's to its template-style design

Mikrotik’s traffic flow supports



Records of Traffic Flow Mikrotik
Mikrotik RouterOS v6.39.1 (stable)

Setup Mikrotik as a Flow Exporter + Server Flow Collector

SETUP MIKROTIK AS A FLOW EXPOTER

```
/ip traffic-flow
set cache-
entries=64k
enabled=yes
interfaces=ether7
```

First, we enabled what interface's going to be exporter the flow records to the flow collector.

```
/ip traffic-flow target
add dst-
address=103.x.y.221
port=600 src-
address=103.x.y.229
version=5
```

Then, set the target of flow collector IP. The default port is 600.

The version flow record that we use is version 5.

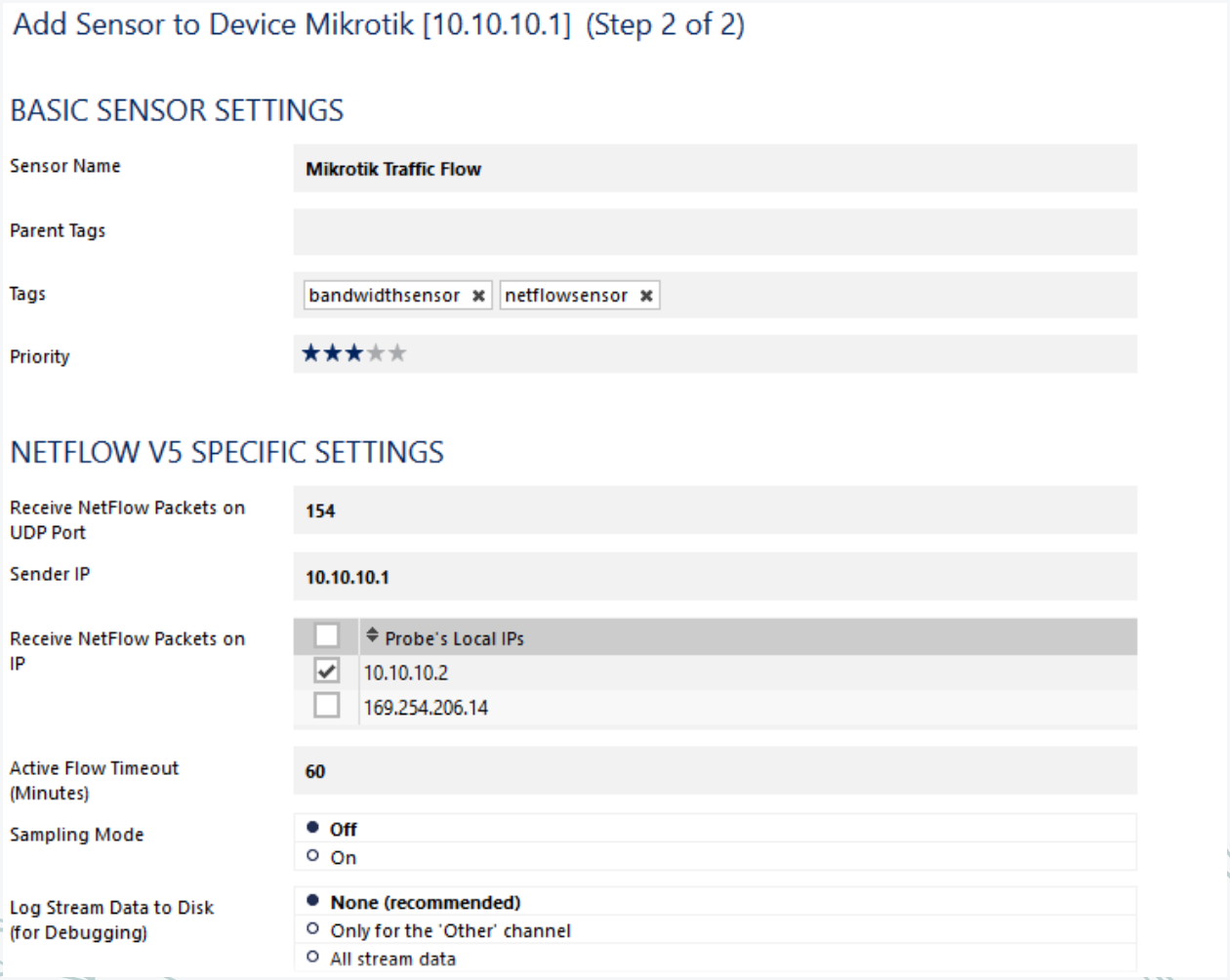
CREATER SERVER AS A FLOW COLLECTOR

In this case, I used PRTG as a Flow Collector with the IP Address 103.x.y.221

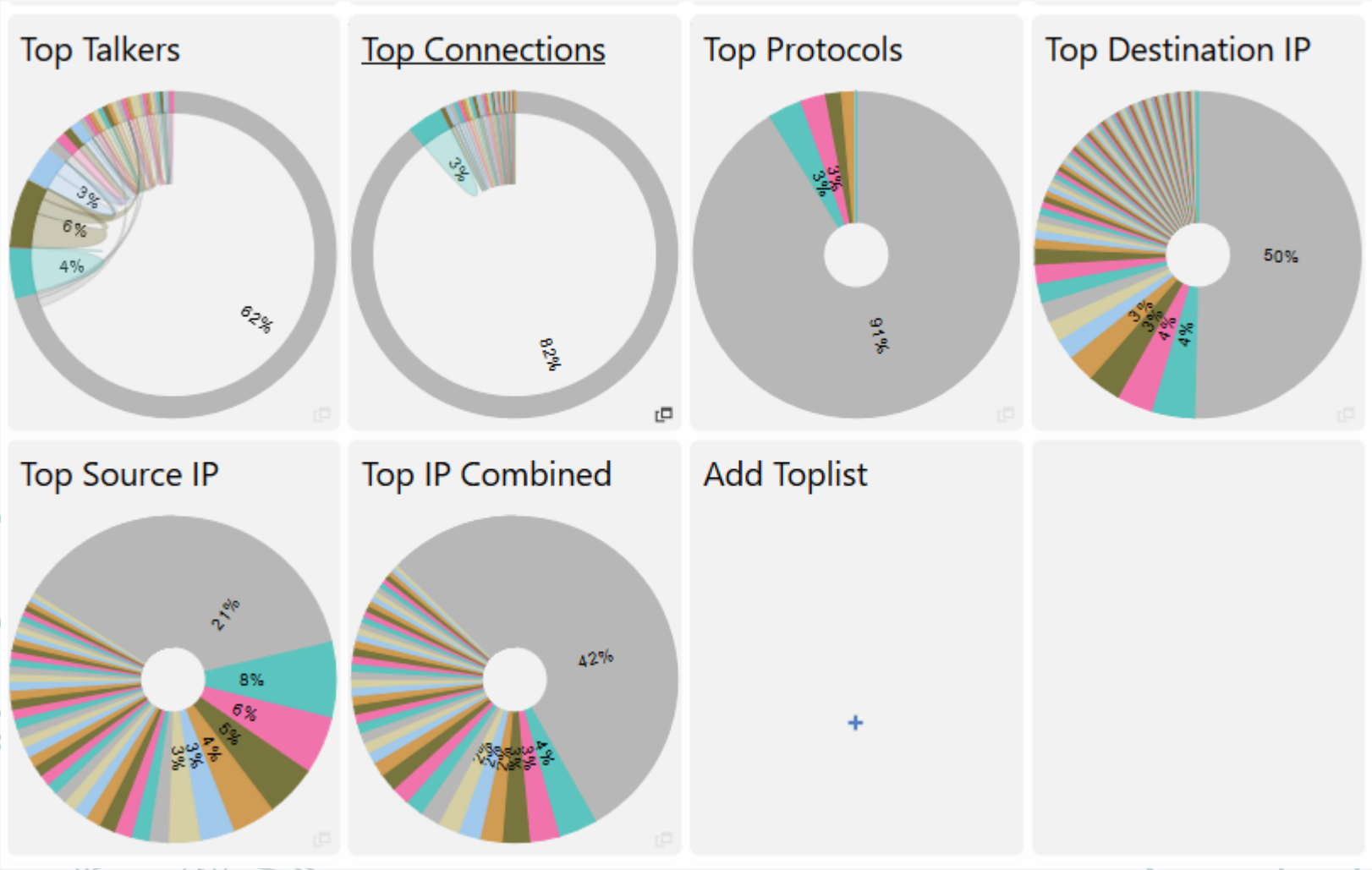
I just activate for src-ip, dst-ip, dst-port, src-port, and protocols

Our firewall allowed port 600 with UDP protocols to network.

SCREENSHOTS



SCREENSHOTS

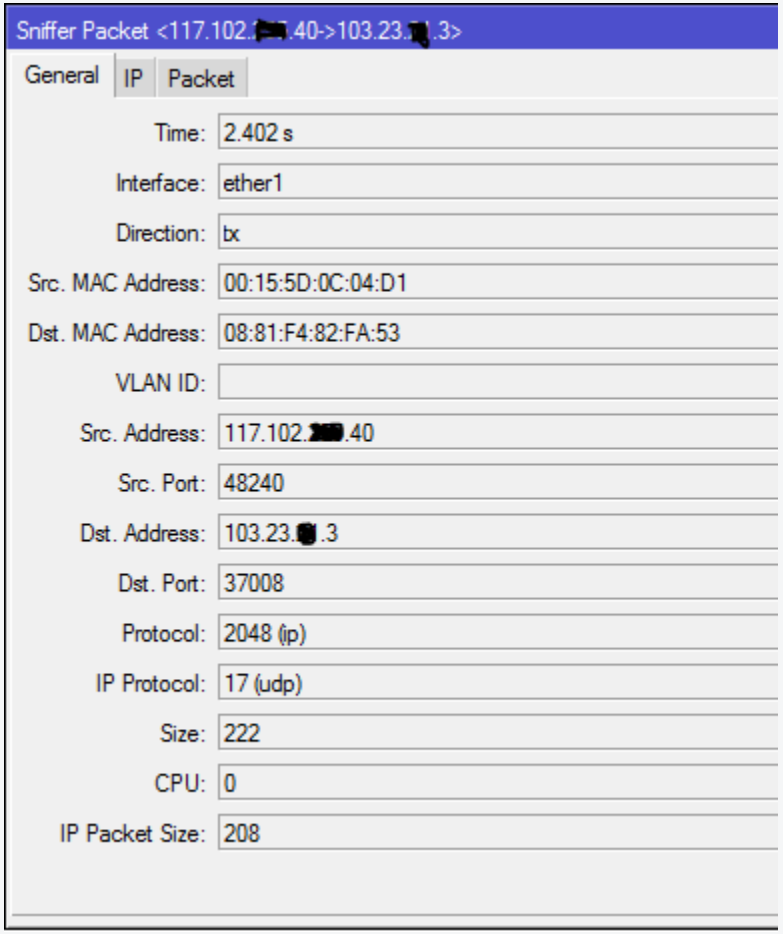


SCREENSHOTS

1 to 50 of 100 — Item Count

Pos	Destination IP	Bytes	
Other		5,338 MByte	50 %
1.	sin11s03-in-f10.1e100.net (172.217.27.42)	440 MByte	4 %
2.	s3-ap-southeast-1-w.amazonaws.com (52.219.40.32)	415 MByte	4 %
3.	sin11s04-in-f106.1e100.net (172.217.27.106)	318 MByte	3 %
4.	sin11s02-in-f10.1e100.net (172.217.27.10)	267 MByte	3 %

SCREENSHOTS




Traffic
International Router
International Limiter
Traffic
International Router
International Limiter
Distribution Router
Local Router
(OpenIXP)
Local Limiter
MacBook Air

How do we use TRAFFIC FLOW AS A DDOS DETECTOR

We’re still researching it ☺

OUR THOUGHT THE PROCESS

Thanks!

Any questions?

You can find me at:

 @isapangestu

 Isa Pangestu

 Cerpen.isapangestu.id

 Isa.Pangestu@outlook.com

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash