

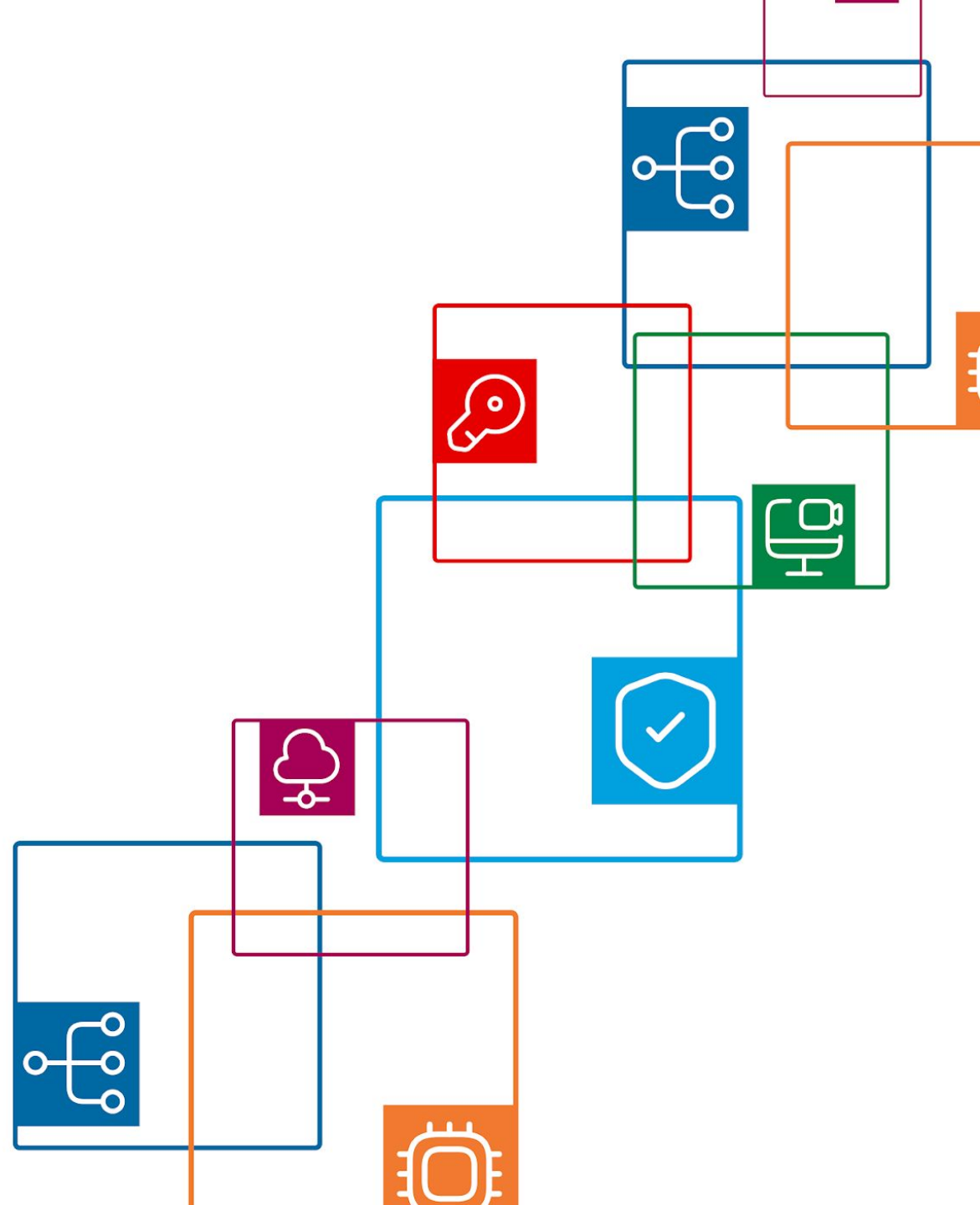


Suriconf

konfigurační asistent Suricata

Eliška Červinková

(eliska.cervinkova@cesnet.cz)



1. Suricata

- ❑ open-source IDS/IPS systém
- ❑ manuální konfigurace Suricata
- ❑ myšlenka - konfigurační asistent

2. Suriconf

- ❑ automatizace konfigurace Suricata
- ❑ Suriconf (verze 1.0.1-dev.2)
- ❑ testování Suriconfu
- ❑ ukázka Suriconfu



Eliška Červinková

GitHub: [<https://github.com/KEIAHNY>]

LinkedIn: [www.linkedin.com/in/eliskacervinkova]



Suricata IDS/IPS

- ❑ open-source IDS/IPS systém
- ❑ výkon Suricaty a její závislosti

Manuální konfigurace

- ❑ znalost technologií
- ❑ experimenty a testování

Nápad: Konfigurační asistent

- ❑ SEPTun - Suricata Extreme Performance Tuning guide
- ❑ Suricata-Test-Suite

Suricata is far more than an IDS/IPS



Source: Stamus Networks

Suriconf

- ❑ přehled
- ❑ statická konfigurace
 - ❑ prekonfigurační běh
 - ❑ dotaz a spuštění
- ❑ závislosti modulů
- ❑ výsledek Suriconfu

Moduly

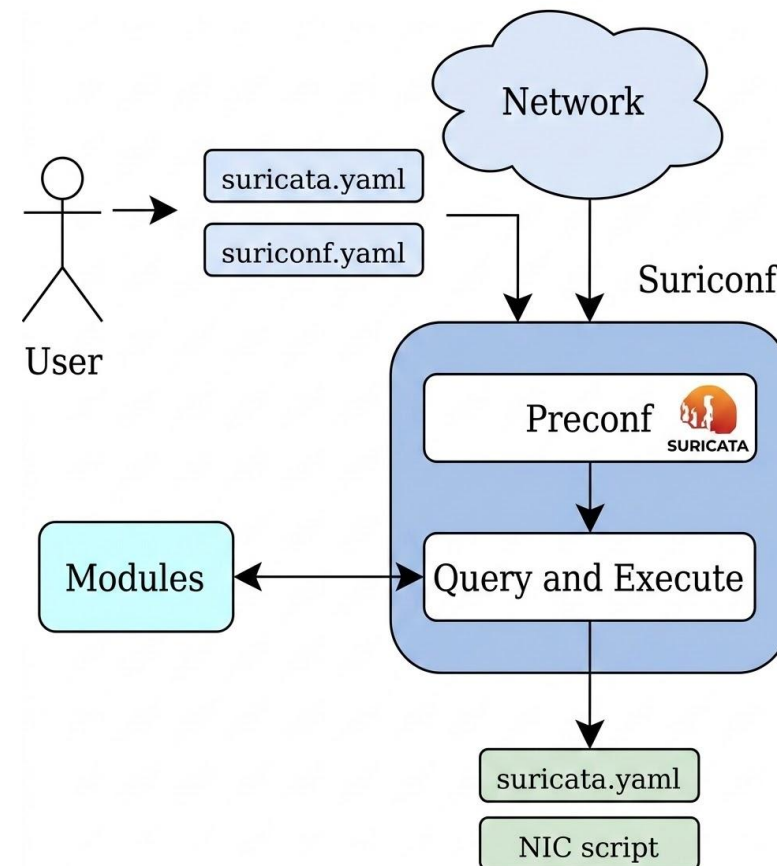
- ❑ CPU affinity
- ❑ Flow threads
- ❑ Flow
- ❑ Memory usage

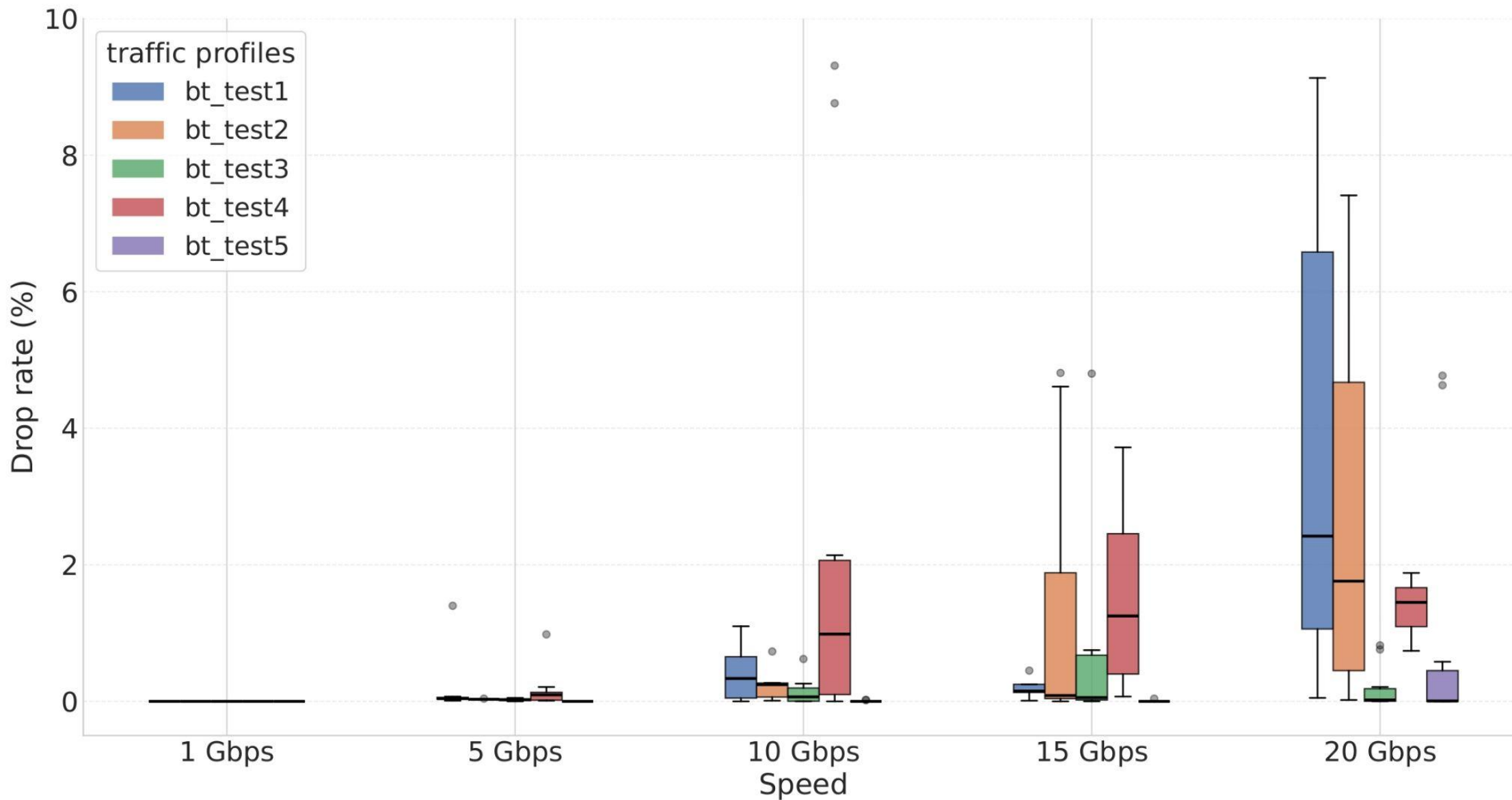
```
%YAML 1.1
---
suriconf-version: 1.1.0-dev
suri-configuration: suricata.yaml
suricata-bin: /usr/bin/suricata
ethtool-bin: /usr/sbin/ethtool
ip-bin: /usr/sbin/ip
log-dir: /var/log/suricata/
socket: /var/run/suricata/suricata-command.socket
preconf-time: 360 # in seconds
# 360 is minimum for flow_threads module
analysis: static # static/dynamic

mode:
  modify:
    enabled: true
    yaml_change: force # ask/force
  suggestion:
    enabled: false

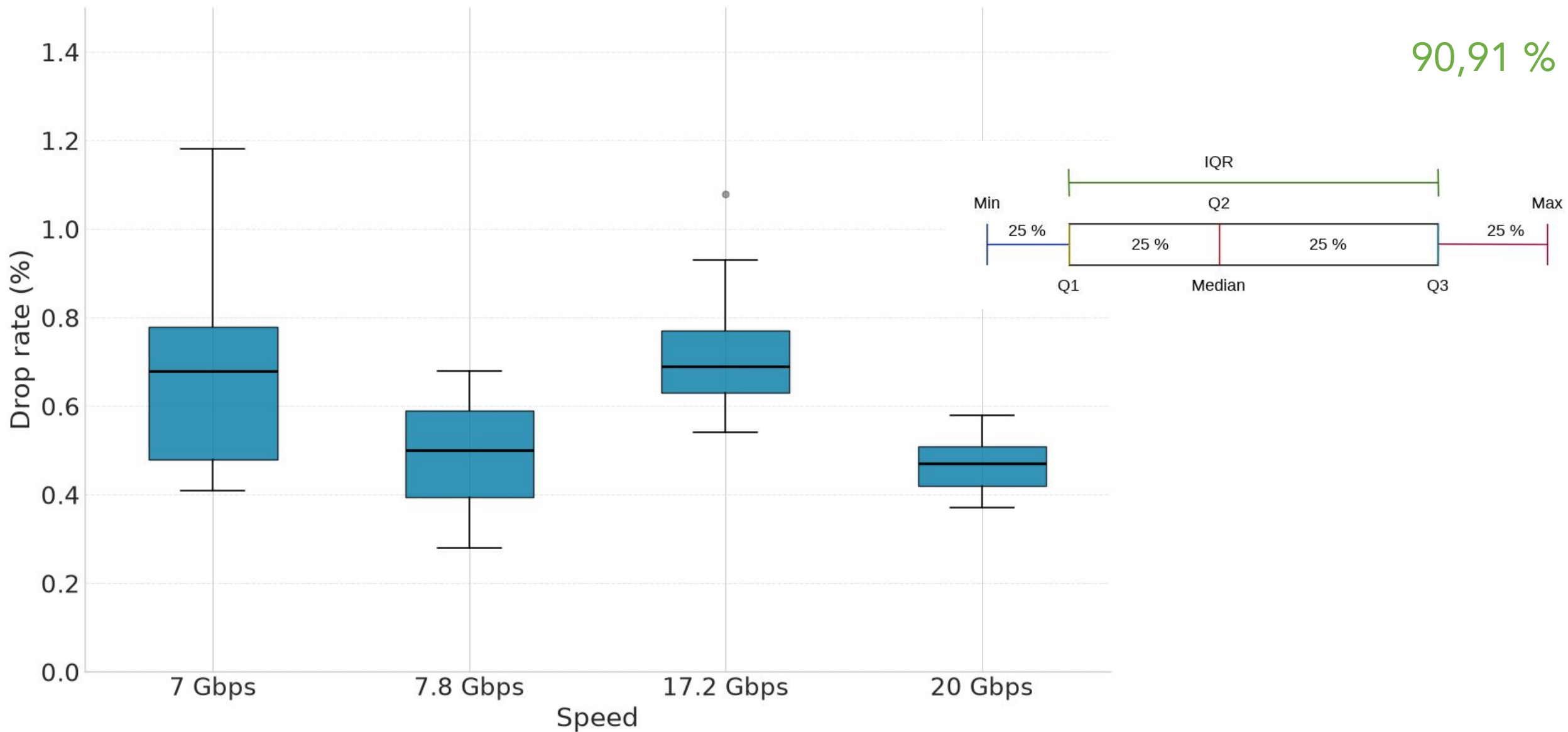
modules:
  - name: cpu_affinity
    enabled: true
  - name: memory_usage
    enabled: true
  - name: flow
    enabled: true
  - name: flow_threads
    enabled: true

variables:
  interface: eth0
  capture_mode: af_packet # dpdk
  max_memory_usage: 1 GiB
  max_cpu_usage_vec: [0-2] # [0-6]
```





80.8 %



Suriconf

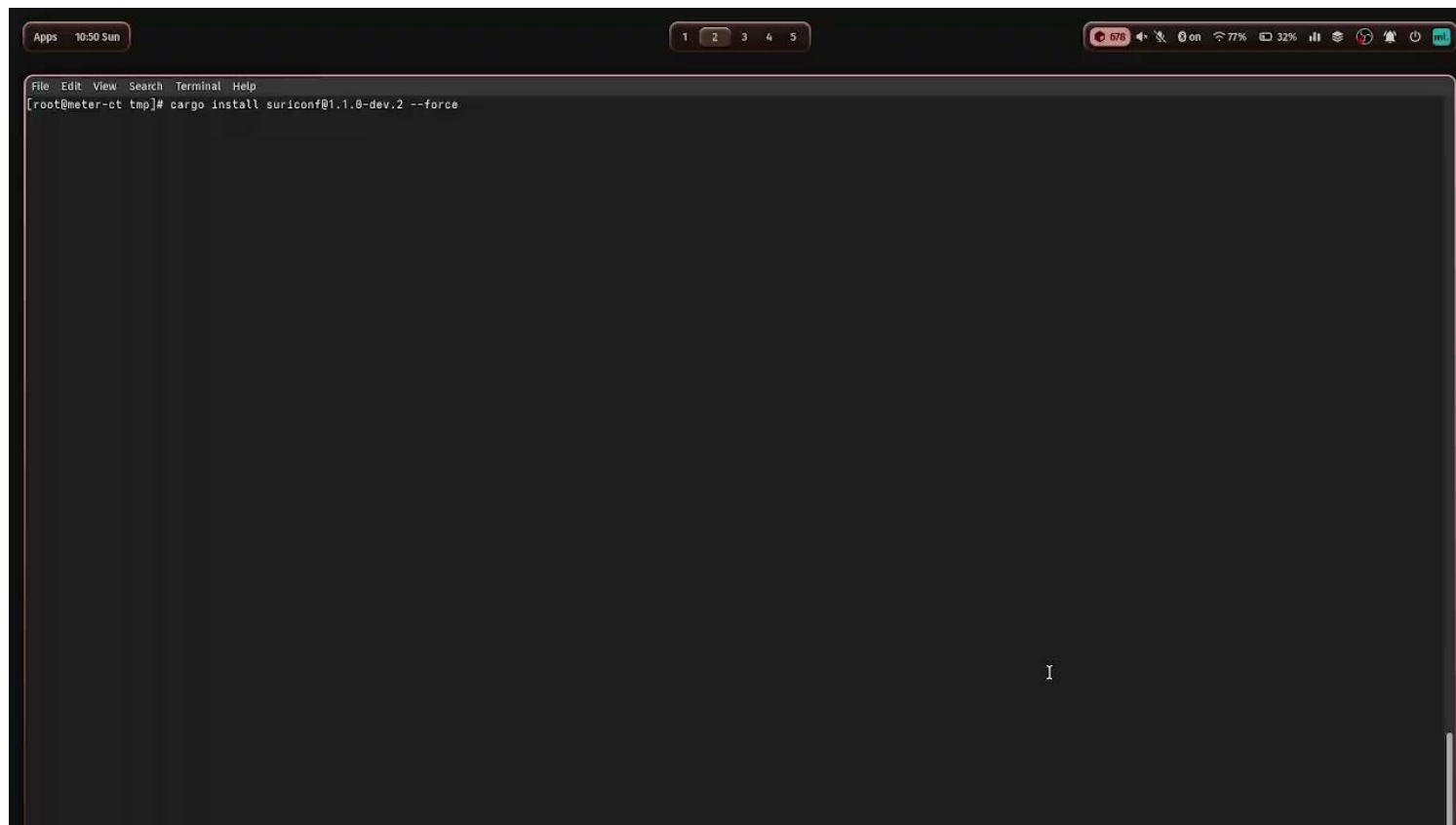
- ❏ `git am ippair-host-defrag-counters.patch`
- ❏ `cargo install suriconf@1.1.0-dev.2`
- ❏ `suriconf init && ls`
- ❏ `./suriconf -c suriconf.yaml`

Suriconf v1.1.0-dev.2:

<https://github.com/CESNET/Suriconf>

result:

<https://github.com/CESNET/Suriconf/blob/ld/result>



The screenshot shows a terminal window with a dark background. The title bar at the top indicates 'Apps 10:50 Sun'. The terminal content shows the command `[root@meter-ct tmp]# cargo install suriconf@1.1.0-dev.2 --force` being executed. The cursor is positioned at the end of the command line. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The system status bar at the top right shows '678', 'on', '77%', and '32%'.

Otázky?

