Mitigating NIDS Saturation through Packet Pre-Filtering using PDP devices

Henrique B. Brum[1,3]
hbeckerbrum@fbk.eu

Luís A. D. Knob[1]
l.diasknob@fbk.eu

Tiago C. Ferreto[2]
tiago.ferreto@pucrs.br

Domenico Siracusa[3]
domenico.siracusa@unitn.it

[1]Center for Cybersecurity, FBK - Fondazione Bruno Kessler, Trento - Italy
[2]School of Technology, PUCRS - Pontifical Catholic University of Rio Grande do Sul, Brazil
[3]Department of Information Engineering and Computer Science, University of Trento, Italy

Introduction

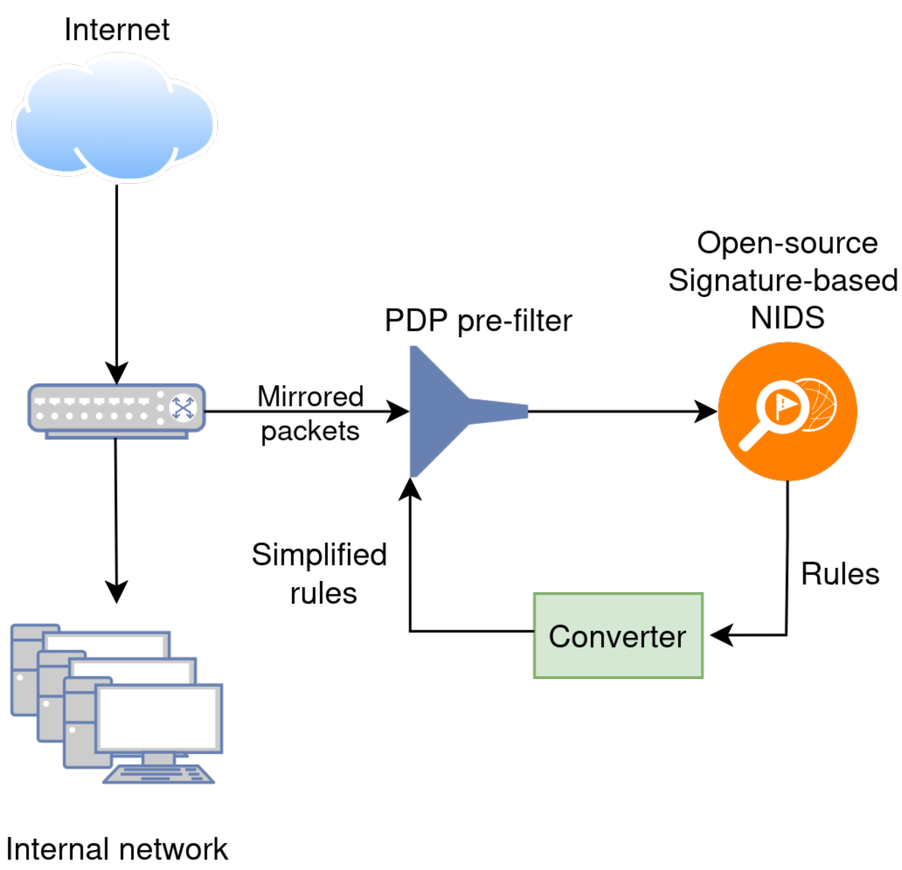
Signature-based network intrusion detection systems (NIDSs) are essential for network protection but can be overwhelmed by the ever-increasing network traffic, leading to saturation and missed attacks. This growing network traffic has driven the adoption of the Programmable Data Plane (PDP) paradigm for its high-speed packet processing capabilities.

- This work proposes mitigating NIDS saturation by **pre-filtering packets** using **PDP devices**
- Offload a simplified version of the NIDS's rules to a PDP device, ensuring only suspicious packets reach the NIDS while filtering out benign traffic

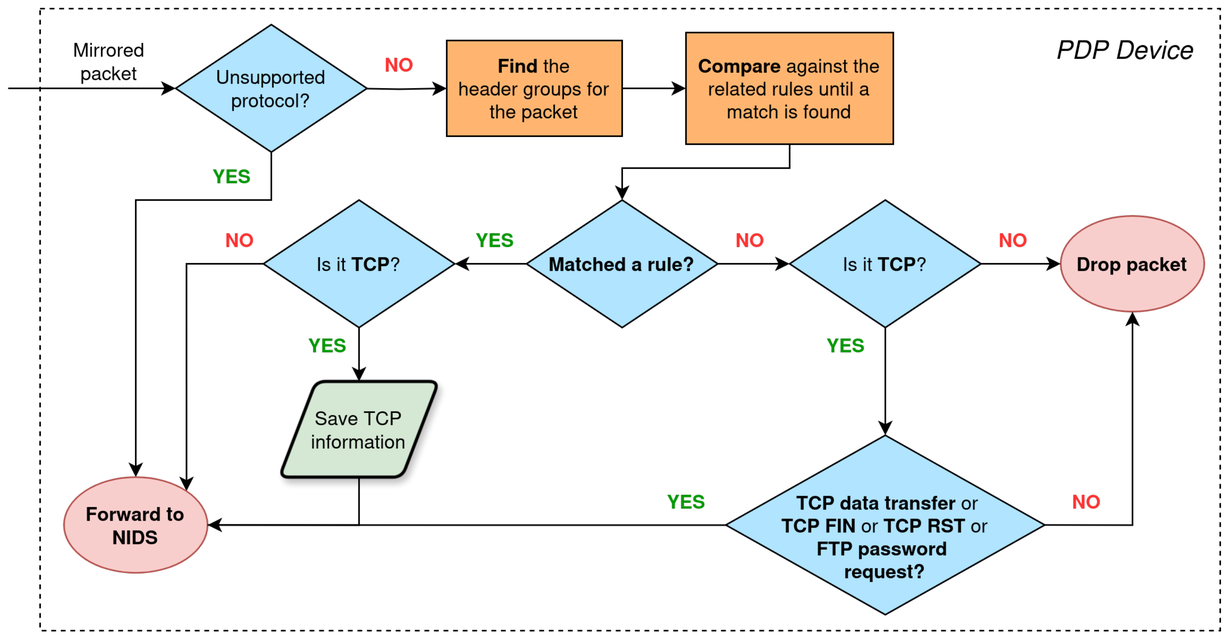
Related Work

- **Flow sampling** [1] is simple but struggles to balance traffic reduction with attack detection
- **Rule-based pre-filtering** [2, 3] achieves a better balance, but existing solutions have failed to integrate with commercial NIDS TCP requirements

Deployment scenario



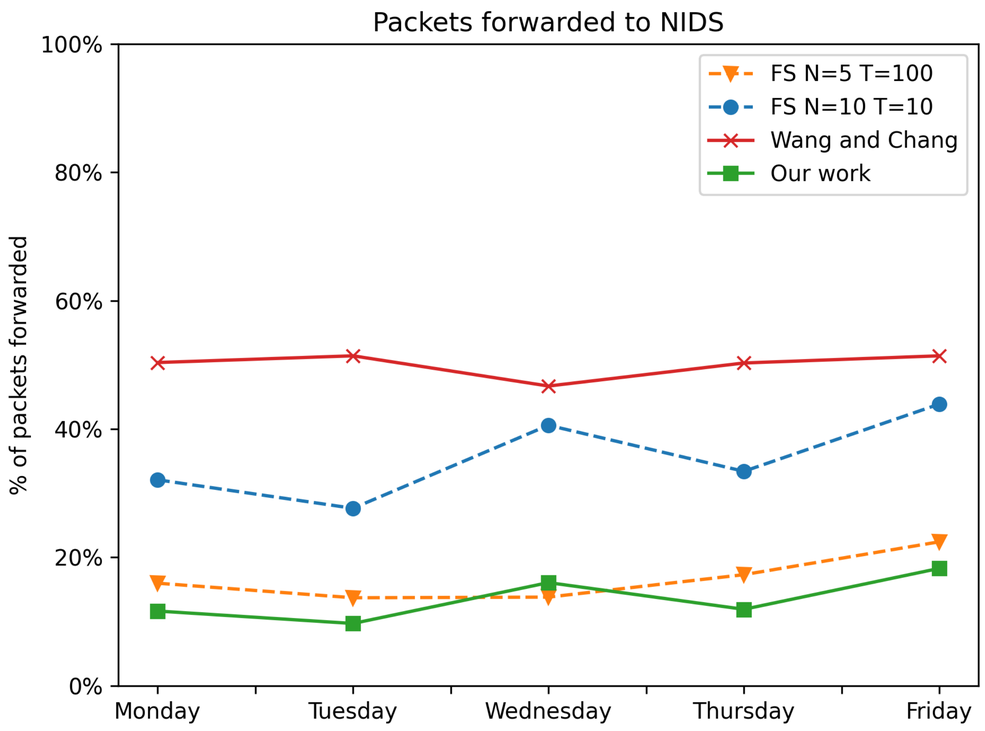
PDP pre-filter

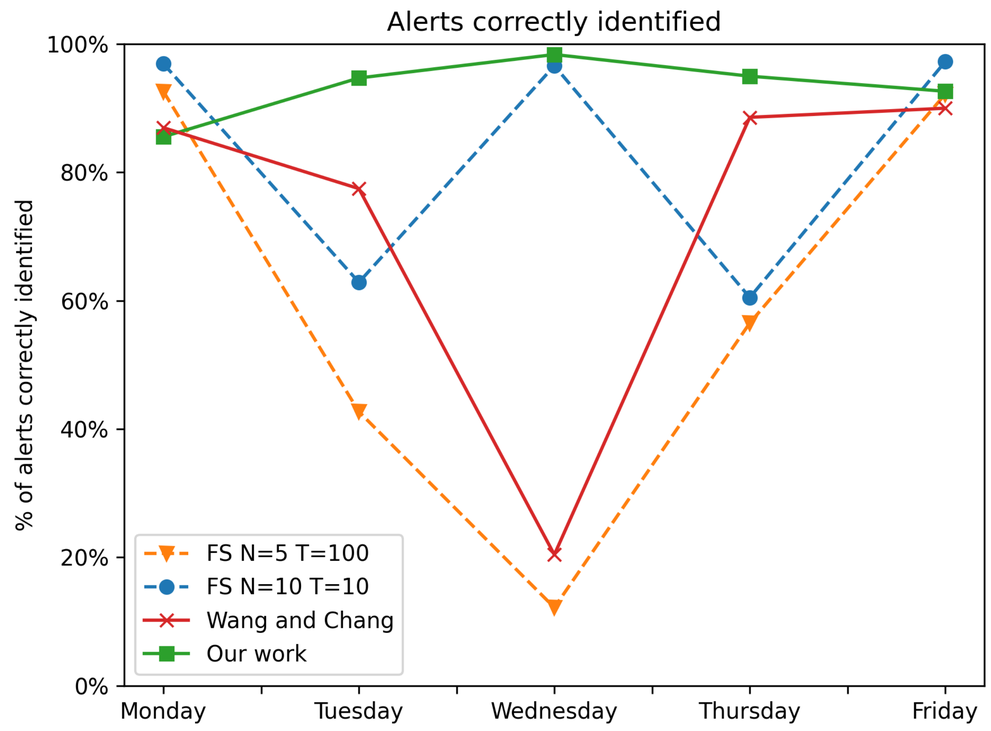


Experiments Setup

- **Python simulator**
- **Snort 3** as the NIDS
- **Snort 3 Registered ruleset**
- **CICIDS2017** as the dataset

Results





Conclusions and Future Work

Our experiments have shown that our work successfully **pre-filters network traffic** while maintaining **high alert detection**. For future work we aim to:

- Support other commercials NIDS, like **Suricata**
- Implement the solution in a real **PDP device**

References

[1] Lewis, Benjamin, et al. "4MIDable: Flexible Network Offloading For Security VNFs." Journal of Network and Systems Management 31.3 (2023): 52.

[2] Wang, Shie-Yuan, and Jen-Chieh Chang. "Design and implementation of an intrusion detection system by using extended BPF in the Linux kernel." Journal of Network and Computer Applications 198 (2022): 103283.

[3] Teofili, Simone, et al. "Ids rules adaptation for packets pre-filtering in gbps line rates." Trustworthy Internet (2011): 303-316.