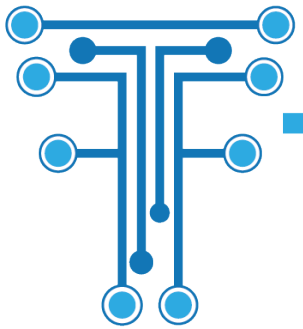


TeraFlow

ML-based attack detector for Teraflow-OS

Prof. Dr. Alberto Mozo (Technical University of Madrid)
joint work with Telefonica, Chalmers University and CTTC

Grenoble, France. 7-10 June 2022

This project has received funding from the European Union's H2020 research and innovation programme under the grant agreement No. 101015857

Teraflow objectives

TeraFlow

Teraflow controller: Secured autonomic traffic management of a Tera of SDN Flows

Adoption of SDN by Telecom Operators

Handle a Tera of flows

Easily integrate with distributed computing through Transport Network Slices

Secure Operator Network

AI/ML based on

- ETSI ZSM
- ETSI ENI

Cybersecurity - MouseWorld

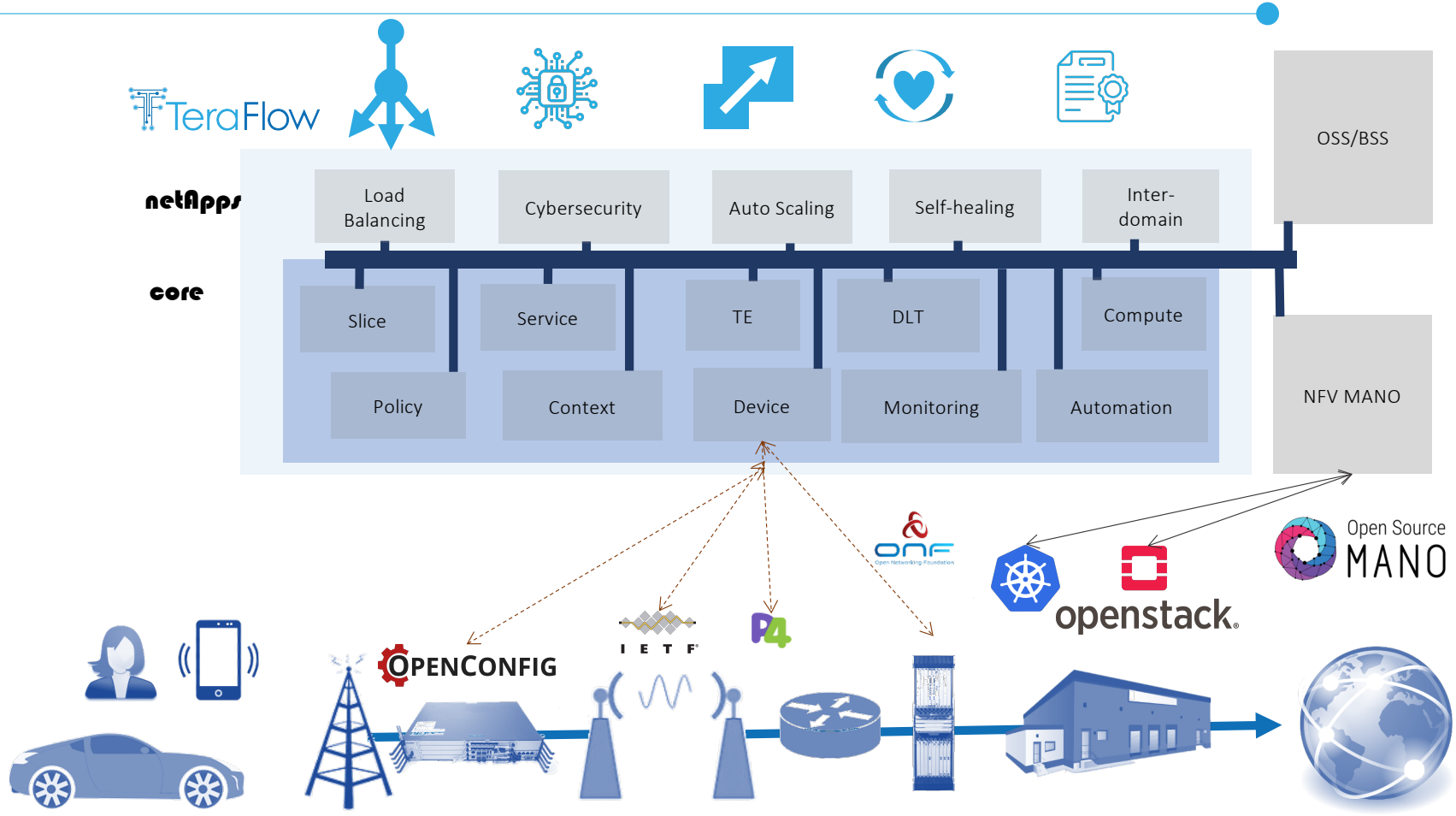
- Attack detection
- Reactive protection
- Synthetic attack generation

ETSI TeraFlowSDN OSG

- **ETSI TeraFlowSDN OSG is the outcome of 5GPPP TeraFlow project.**
- **The ETSI Open Source Group for TeraFlowSDN (OSG TFS) is developing an open source cloud native SDN controller enabling smart connectivity services for future networks beyond 5G.**
- KoM in June 2022. Ricard Vilalta (CTTC) is Chair of Leadership Group.
- TeraFlowSDN has the objective of easing the adoption of SDN by telco operators. We want to bring innovation in the ecosystem and contribute to network programmability for current 5G and beyond deployments.
- TeraFlowSDN will ease proof-of-concept demonstration for many ETSI ISG to demonstrate faster the proposed standard solutions.
- “At Telefónica we are looking to ETSI TeraFlowSDN as a solution that demonstrates the advantages of open and disaggregated networks and allows fast new use cases prototyping. After this important milestone, we are looking forward to work alongside the industry in advancing the carrier grade commercial-ready solutions to be deployed in all our networks.”

  Juan Pedro Fernández Palacios, Telefónica

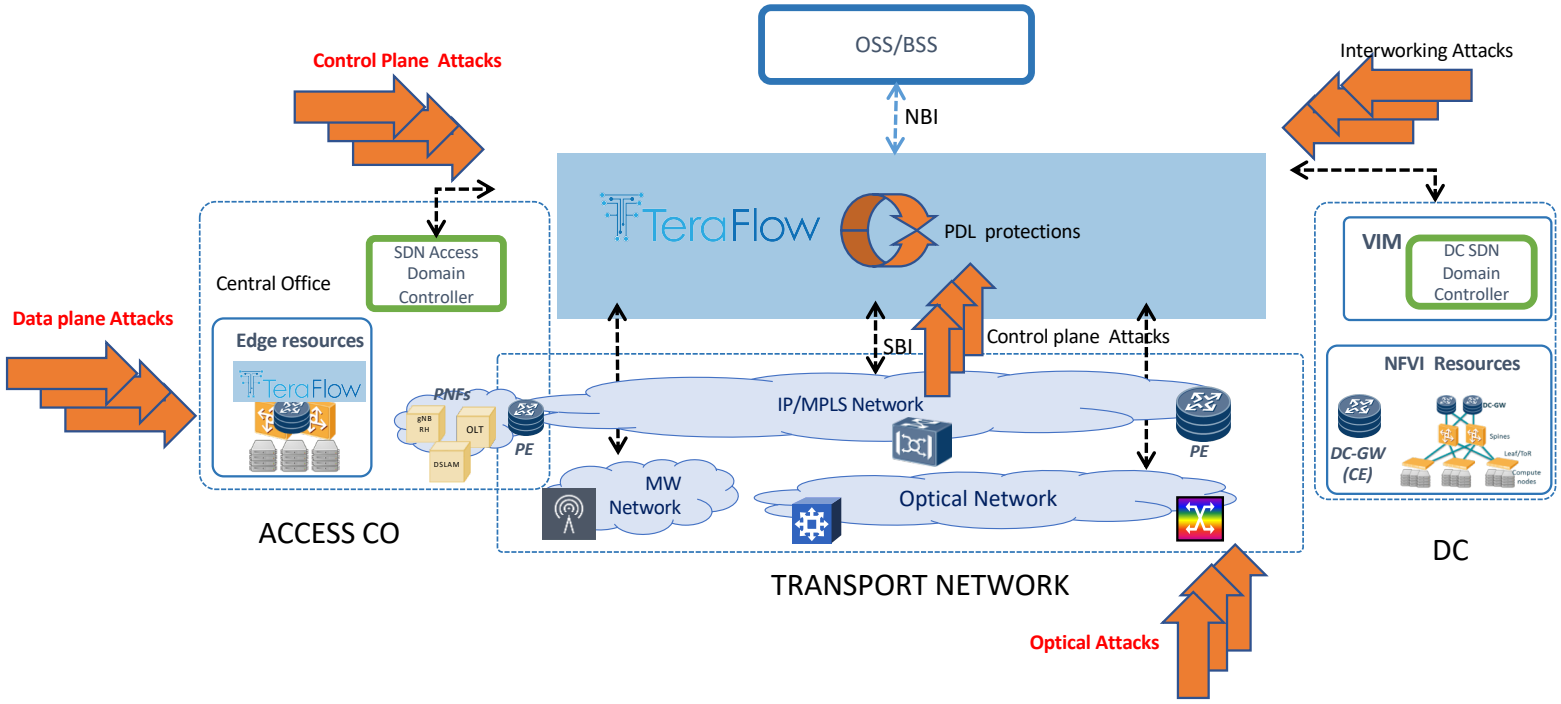
TeraFlow Architecture



Cybersecurity

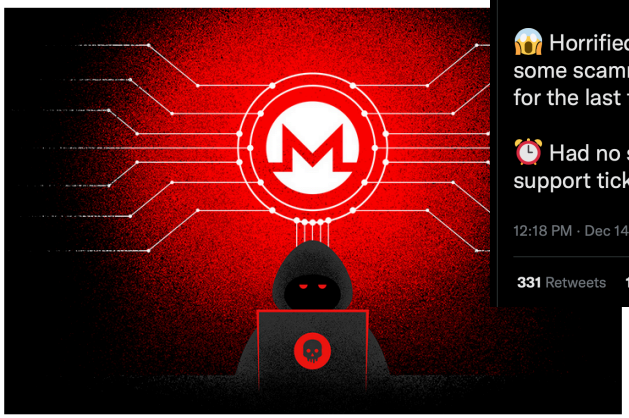
Categories of use cases

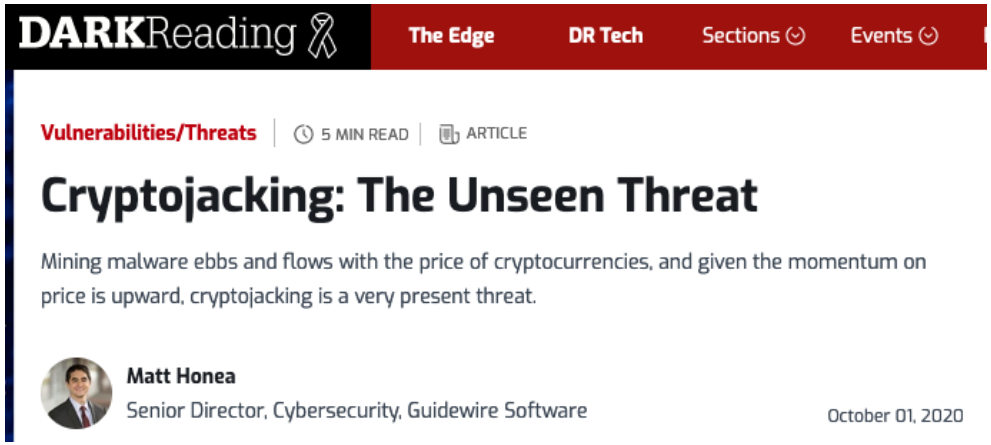
Cyberthreat analysis and protection



Cyberthreat case: Cryptominng today problem

- Not clearly ilegal activity but usually associated with attacks and maliciosus activities
  - Suply chain attacks, malware, insiders (e.g. employees exploitingresources)





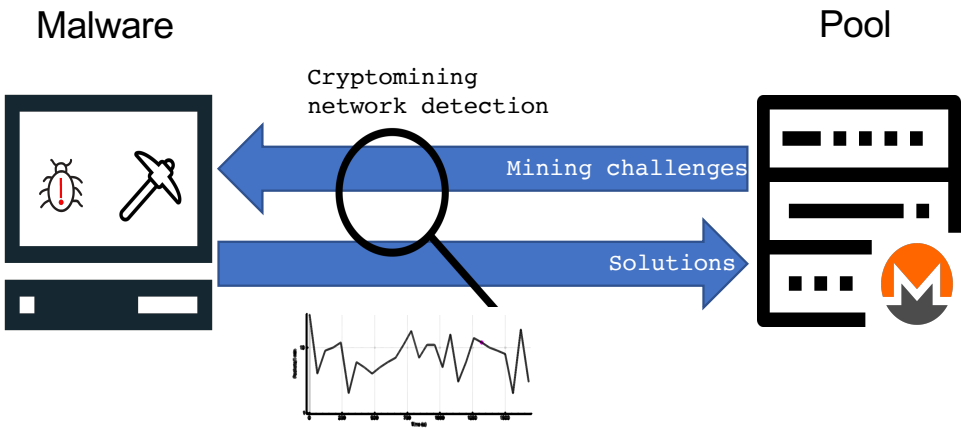
Cryptomining

Cryptomining

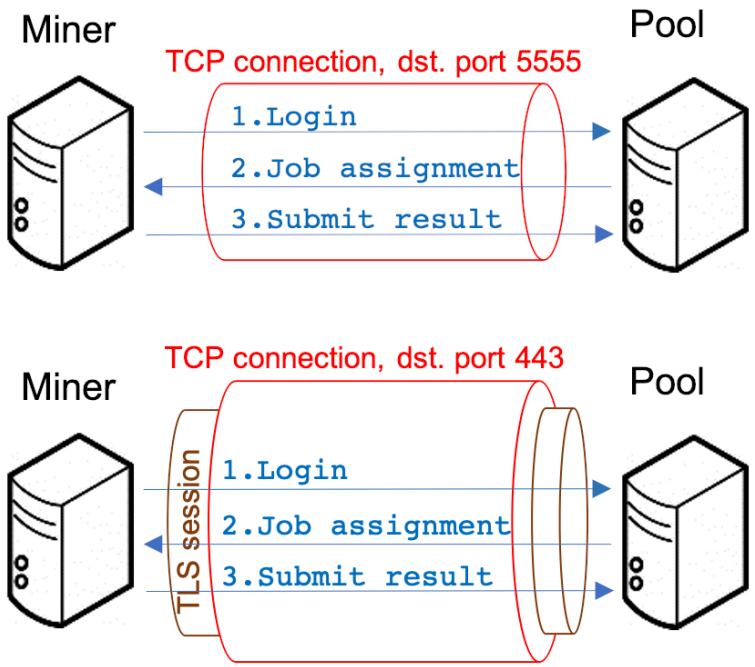
- Use computer resources to make complex calculation to register blocks into currency blockchain. First to complete earn $$$
- Users join efforts to be the first to complete the Job
  - Central server “pool” distribute the job to users (“miners”).
- A network protocol is used

Security problem to solve

- Usually associated to malware
- Power and CPU consumption with impact in processes
- Non easily detected by network IDS:
  - multiples ports
  - Hidden over TLS
  - Destination proxies hide final pool address



Stratum protocol




```
{
 "method": "login",
 "params": {
  "login": "wallet address (hidden)",
  "pass": "xxxxx",
  "rigid": "",
  "agent": "xmr-stak/2.5.1"
 },
 "id": 1
}
```

1.login

```
{
 "method": "submit",
 "params": {
  "id": "9339f59b-d3f5-4a81-9716-2780f6ef8213",
  "job_id": "HXm7DudxRh2CcmCmKc0S+pY/I2LI",
  "nonce": "76f00000",
  "result": "edbc0ce78a558573ac0692b401a0af9a99bdde9e81762809a9faf92766670600"
 },
 "id": 1
}
```

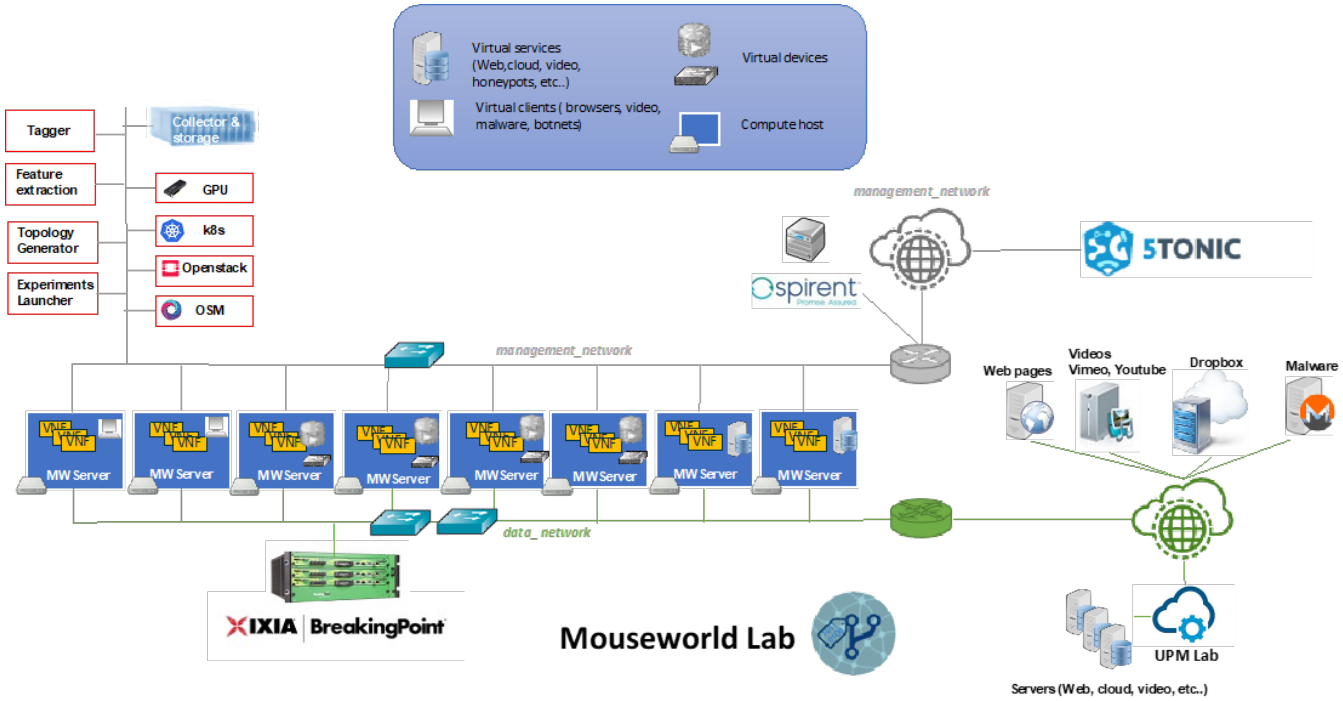
3. Submit result

```
{
 "id": 1,
 "jsonrpc": "2.0",
 "error": null,
 "result": {
  "id": "9339f59b-d3f5-4a81-9716-2780f6ef8213",
  "job": {
   "blob": "0909b6d4c2de0592a2ec37acd4fe2e7a0da2818db78b842588644e87d5d81859ee43ba13173d37000000002ae5ad02a2de88933d06a9d2b1098aaf32b428a3a1415cde0c5e645b858d432c05",
   "job_id": "HXm7DudxRh2CcmCmKc0S+pY/I2LI",
   "target": "b88d0600",
   "id": "9339f59b-d3f5-4a81-9716-2780f6ef8213"
  },
  "status": "OK"
 }
}
```

2.Job assignment

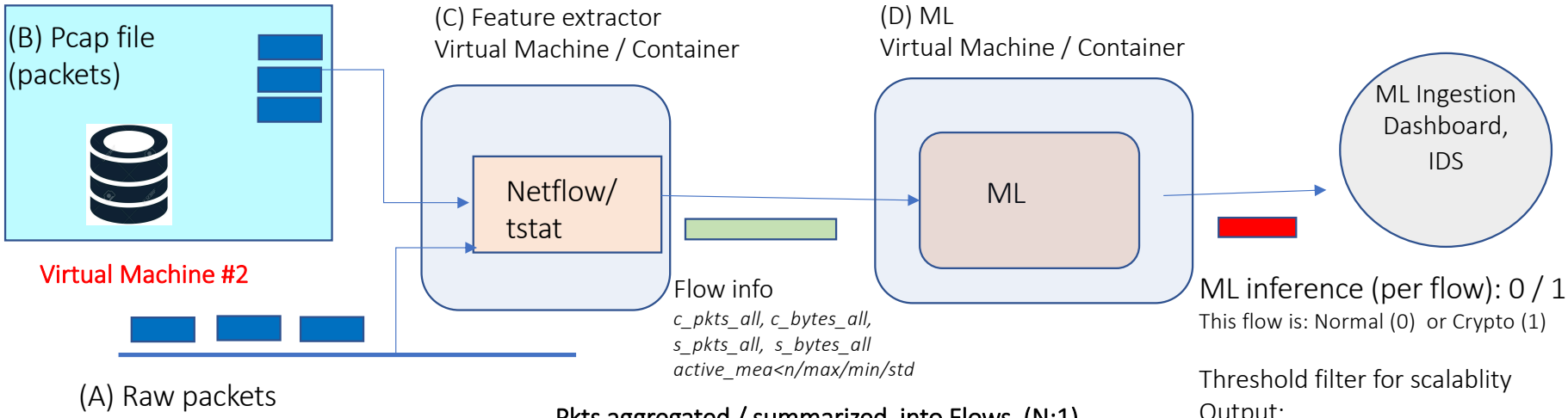
ML development

- Set up of real crytomining clients (linux VMs) interacting with real servers in the Internet
- Data capture (packets)
- Automatic data labelling (connections: normal,crypto)
- ML training and testing
- Packaging of ML algorithm in a dockerized STA (Smart Traffic Analizer)



Pastor, A., Mozo, A.,et al.. (2020). Detection of encrypted cryptomining malware connections with machine and deep learning. IEEE Access

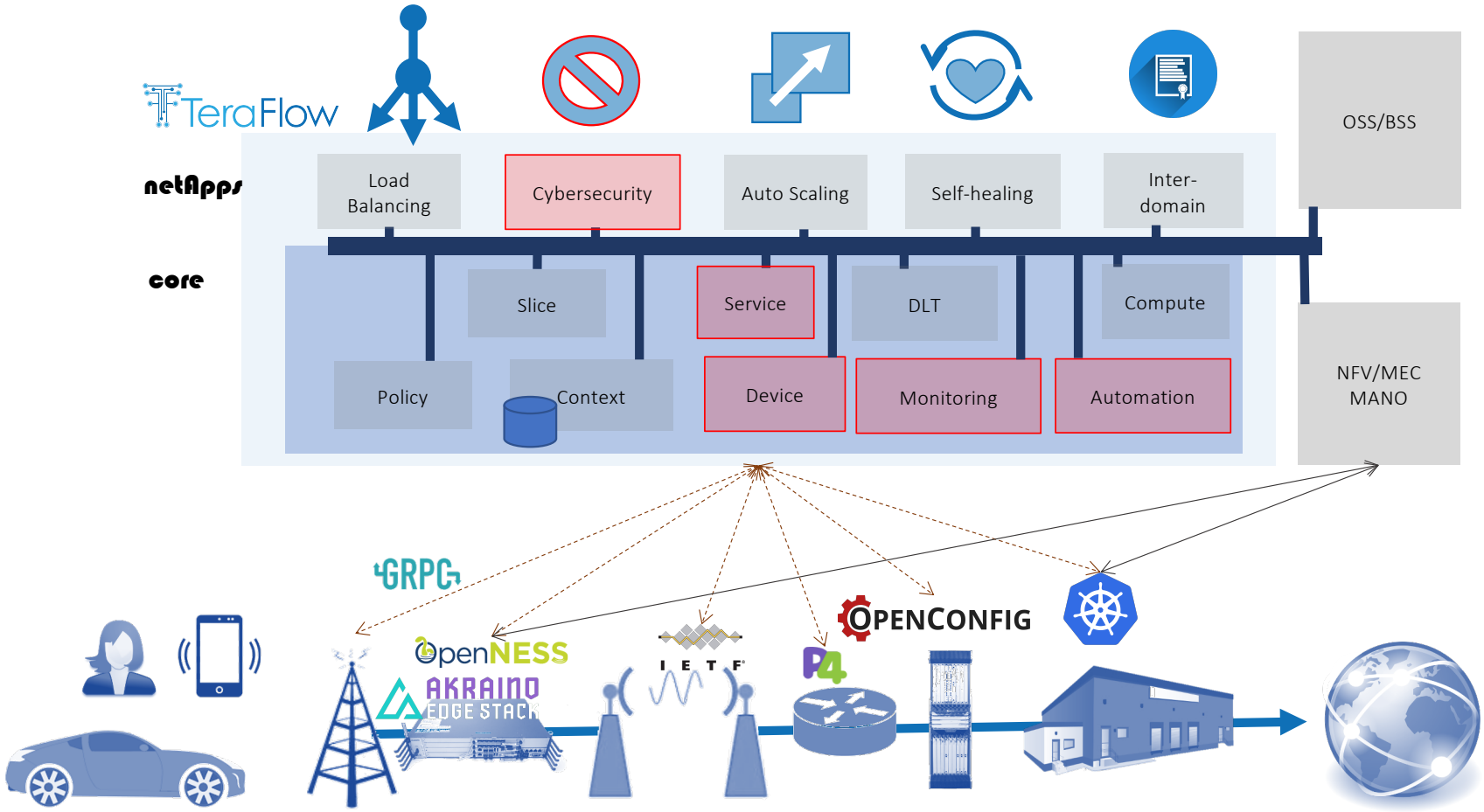
ML deployment



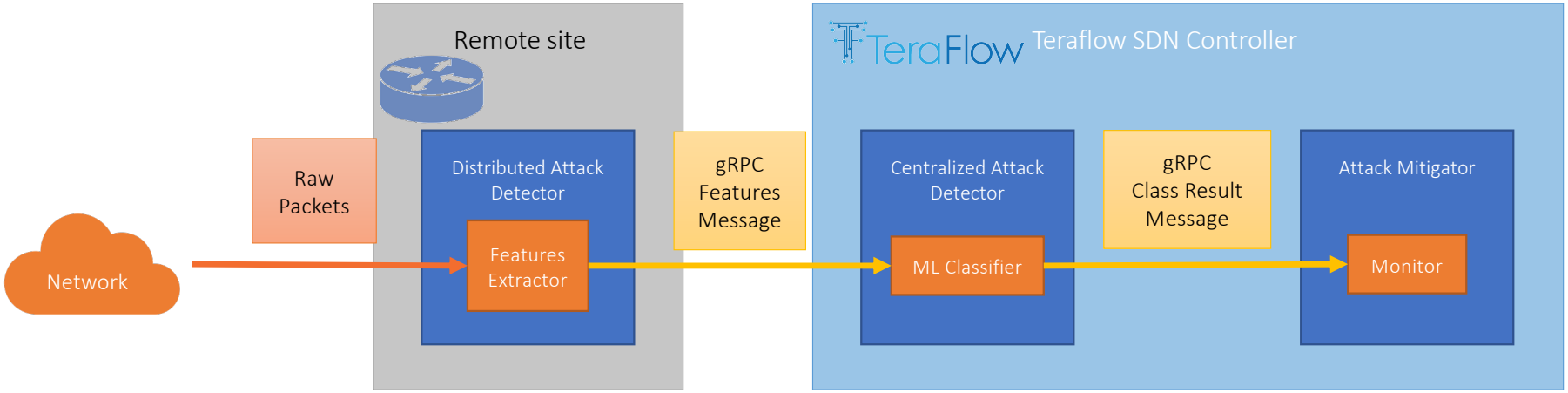
Packet generation
- (B) Re-injection of pcap files
- (A) Normal+ attack + background noise traffic

ML Training and Testing:
- Data gathering/labelling (Mouseworld,offline)
- ML Training &Testing (Mouseworld,offline)
- Real-time testing in Mouseworld-> Teraflow
  - Normal/Attack traffic generation (A)
  - Pcap file re-injection (B)

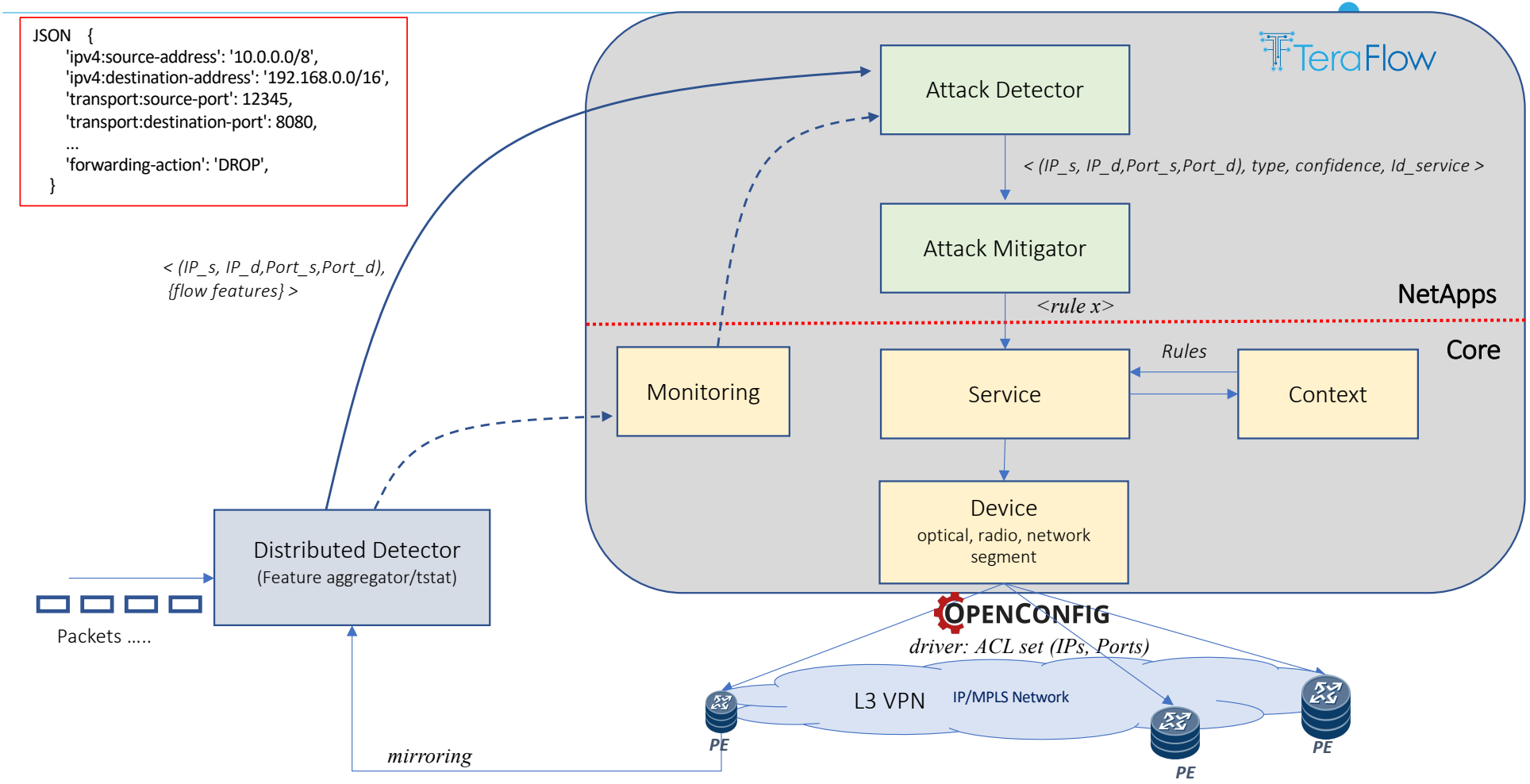
Architecture (cybersecurity)



Distributed attack detector v1.0



Distributed attack detector v2.0



Thank you

Questions?