

# Process level network security monitoring and enforcement with eBPF

SSTIC 2020



**DATADOG**



**Guillaume Fournier**

Security Engineer

[github.com/gui774ume](https://github.com/gui774ume)

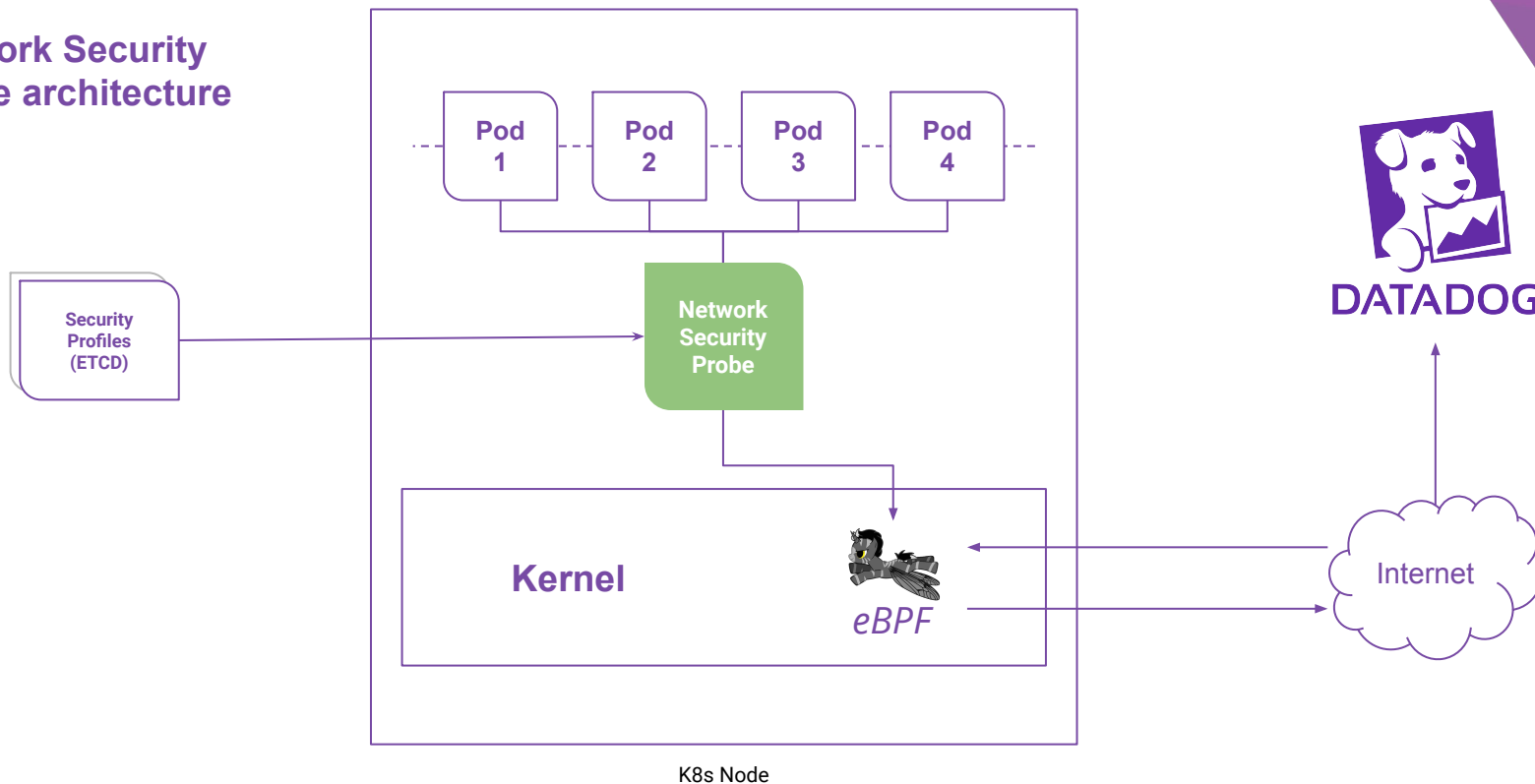
[gui774ume.fournier@gmail.com](mailto:gui774ume.fournier@gmail.com)

# I. Problem   II. eBPF: a new technology   III. Proposal   IV. Demo

- Cutting egress is hard (filtering ports / protocols is not enough)
  - IP based solutions
  - DNS based solutions
- Applying networking rules is hard
  - Granularity
  - Kubernetes (rules propagation & pods scheduling)

**Provide a network access control solution, at the process level, in a Kubernetes environment**

## Network Security Probe architecture





- Cutting egress is hard (filtering ports / protocols is not enough)
  - IP based solutions
  - DNS based solutions

→ Snoops on DNS requests to enforce IPs

- Applying networking rules is hard
  - Granularity
  - Kubernetes (rules propagation & pods scheduling)

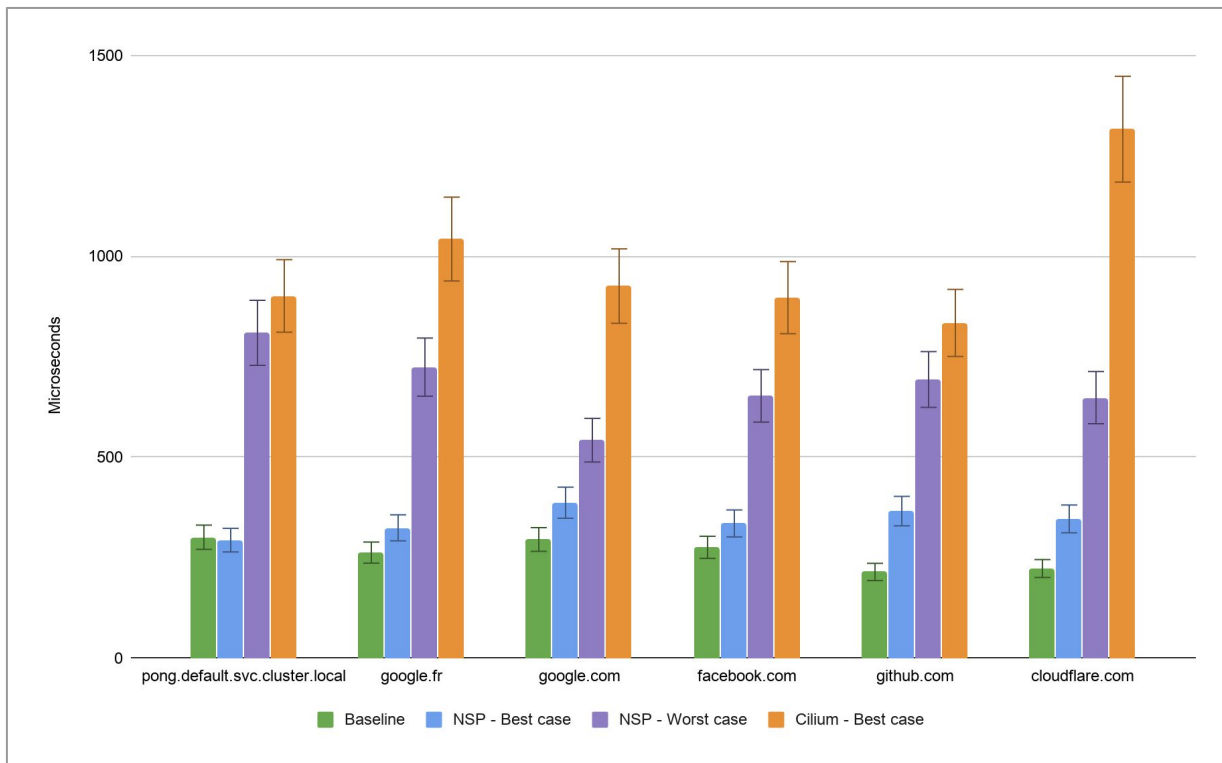
→ Per workload and per process rules



- Differences with Cilium
  - Process level monitoring & enforcement
  - Non-intrusive design
  - In-kernel DNS parsing
  - Attacks detection & prevention
  - Includes host protection



**In-kernel overhead:** Average round trip time per domain (over 5000 A record queries / domain)

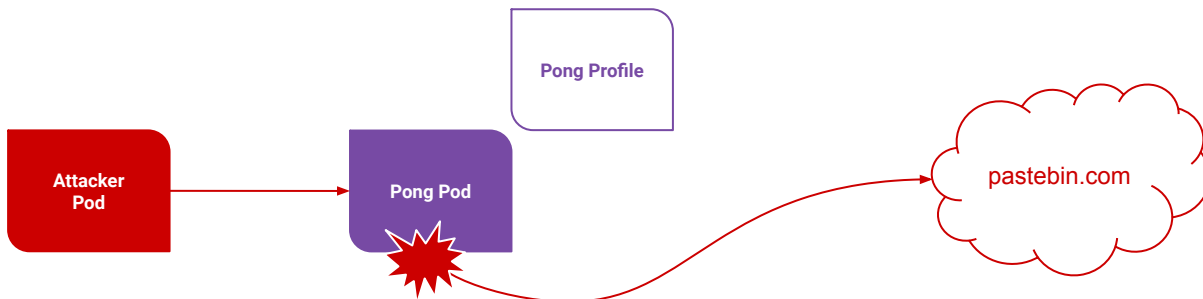


Linux ubuntu-bionic 4.15.0-88-generic, 2 vCPUs Intel Core i7, 8 Gb RAM, minikube version: v1.6.2

# I. Problem   II. eBPF: a new technology   III. Proposal   IV. Demo



Demo 1: security profiles configuration and update



Demo 2: RCE exploitation

# Thanks

Source code:

<https://github.com/gui774ume/network-security-probe>

[guillaume@datadoghq.com](mailto:guillaume@datadoghq.com)