LF NETWORKING
Developer & Testing Forum

L3AF Project Update

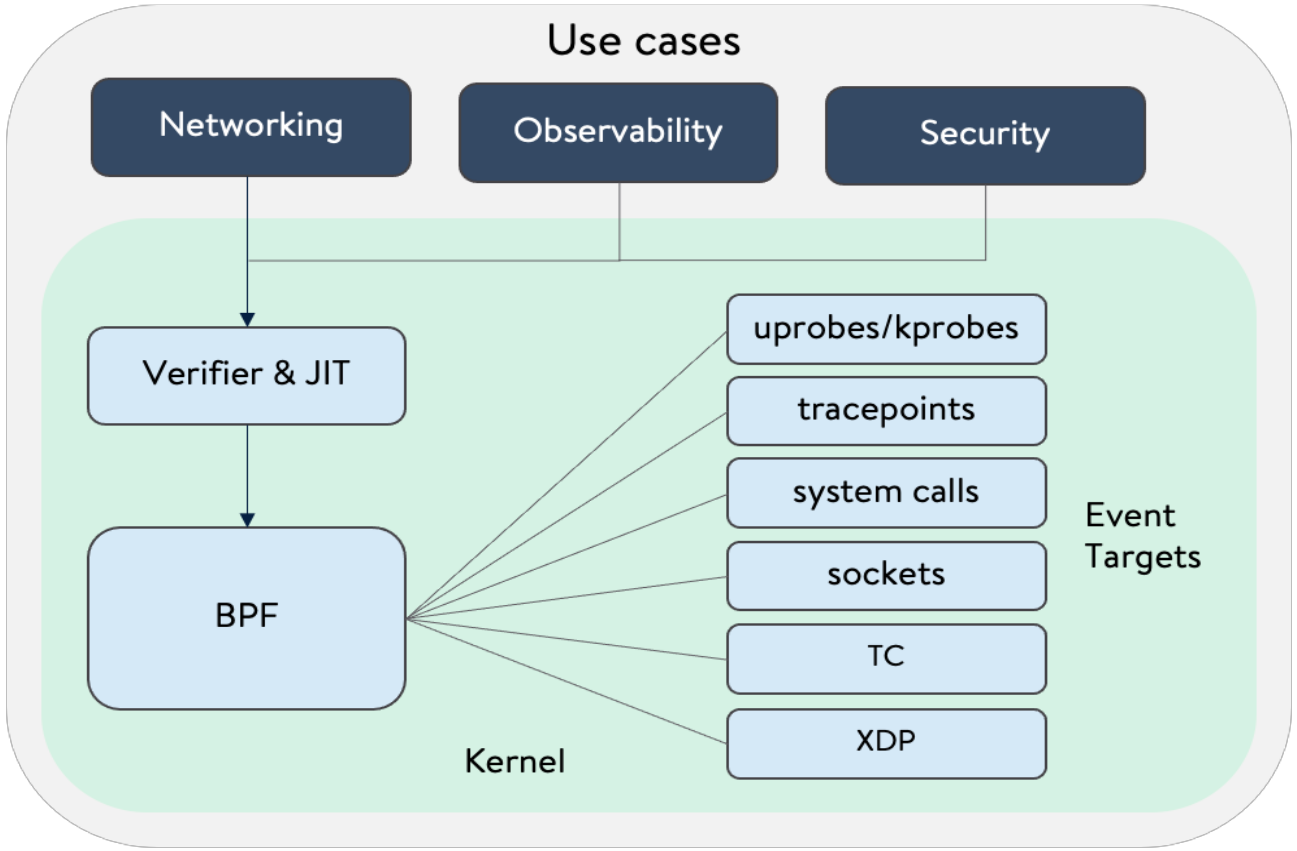
Santhosh Fernandes & Jay Sheth
Walmart Global Tech
https://l3af.io

Agenda

- Introduction to eBPF
- Introducing L3AF
- L3AF Platform
- R1 Release
- R2 Roadmap
- Traffic Mirroring Tool
- Demo
- Q&A

Introduction to eBPF

Sandboxed environment to insert code into the running kernel



eBPF Awesomeness

- ✓ Speed and Performance
- ✓ Safe and secure runtime
- ✓ Event driven
- ✓ Dynamic Programmability

Market Adoption

- ✓ Facebook, Netflix, Cloudflare and other top global companies have developed eBPF/XDP based solutions
- ✓ Open-Source CNIs like Cilium and Calico leverage eBPF to define and manage network/app security policies

L3AF: Introduction

LFN NETWORKING
LFN Developer & Testing Forum

Innovation

Industry's first "eBPF Program-as-a-Service"

Multiple independent programs executing in a chain

More to come, including a community-driven eBPF Package Repository

L3AF

Complete Lifecycle Management of **eBPF programs in the Kernel**

Empowerment

Simple API to add, remove, and reorder eBPF programs on the fly

Configurable metrics are gathered for each eBPF programs

Replace proprietary applications and hardware with blazing fast eBPF code

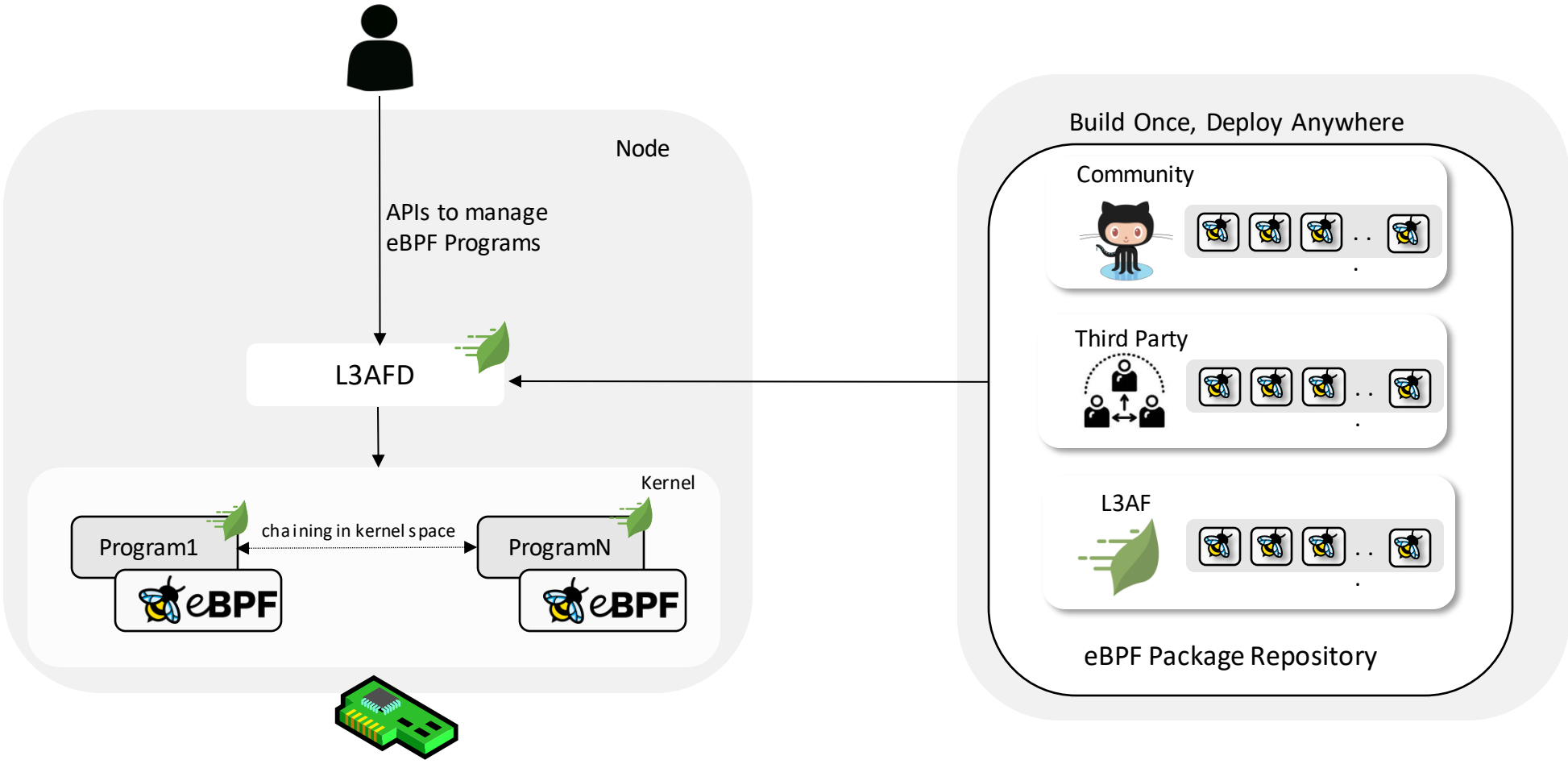
Flexibility

Distributed model to manage and configure eBPF Programs on a per-node basis

Compose eBPF Package Repository to fit business needs

Cloud and vendor agnostic

L3AF: Platform



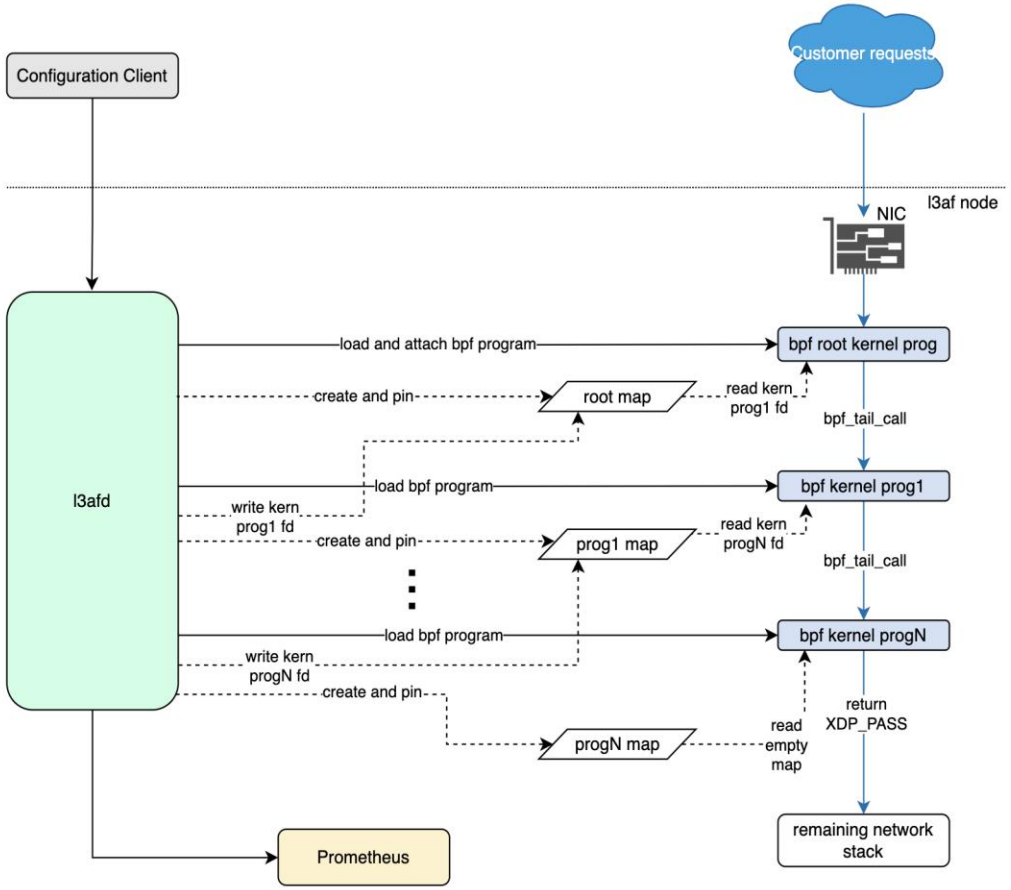
L3AF: R1 Release

- mTLS support for protecting REST APIs
- New REST APIs for adding and removing eBPF programs
- Support file and http(s) eBPF package repositories and overriding default repo for each eBPF program
- CI/CD pipeline improvements (CodeQL, OpenSSF scorecard, Dependabot, staticcheck)

https://github.com/l3af-project/l3afd/releases/tag/v1.0.0

L3AF: R2 Roadmap

- Improve eBPF loading and chaining
- Native loading of eBPF program(s) into the kernel using go library (Cilium/eBPF)
- Implement Chaining using tailf with Cilium library
- XDP support for Windows
- L3AFD running on Azure Windows



https://github.com/orgs/l3af-project/projects/3

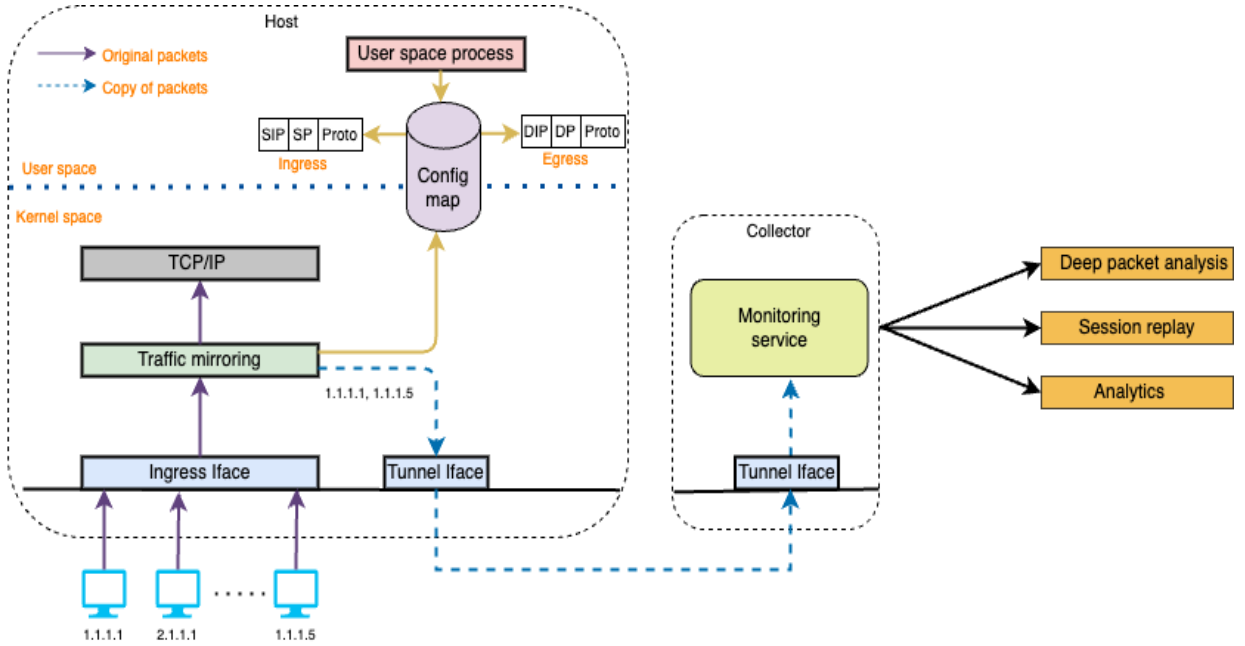
L3AF: eBPF-Package-Repository

- Modify existing eBPF programs (tc-root, xdp-root, ratelimiting, connection limiting, and ipfix flow exporter) for l3afd R2 native go chaining
- Remove hard coding of map paths in eBPF programs
- Support BPF CO-RE to improve eBPF compatibility on Linux

https://github.com/l3af-project/l3af-arch/discussions/39#discussioncomment-4160891

Traffic Mirrorring Tool (TMT)

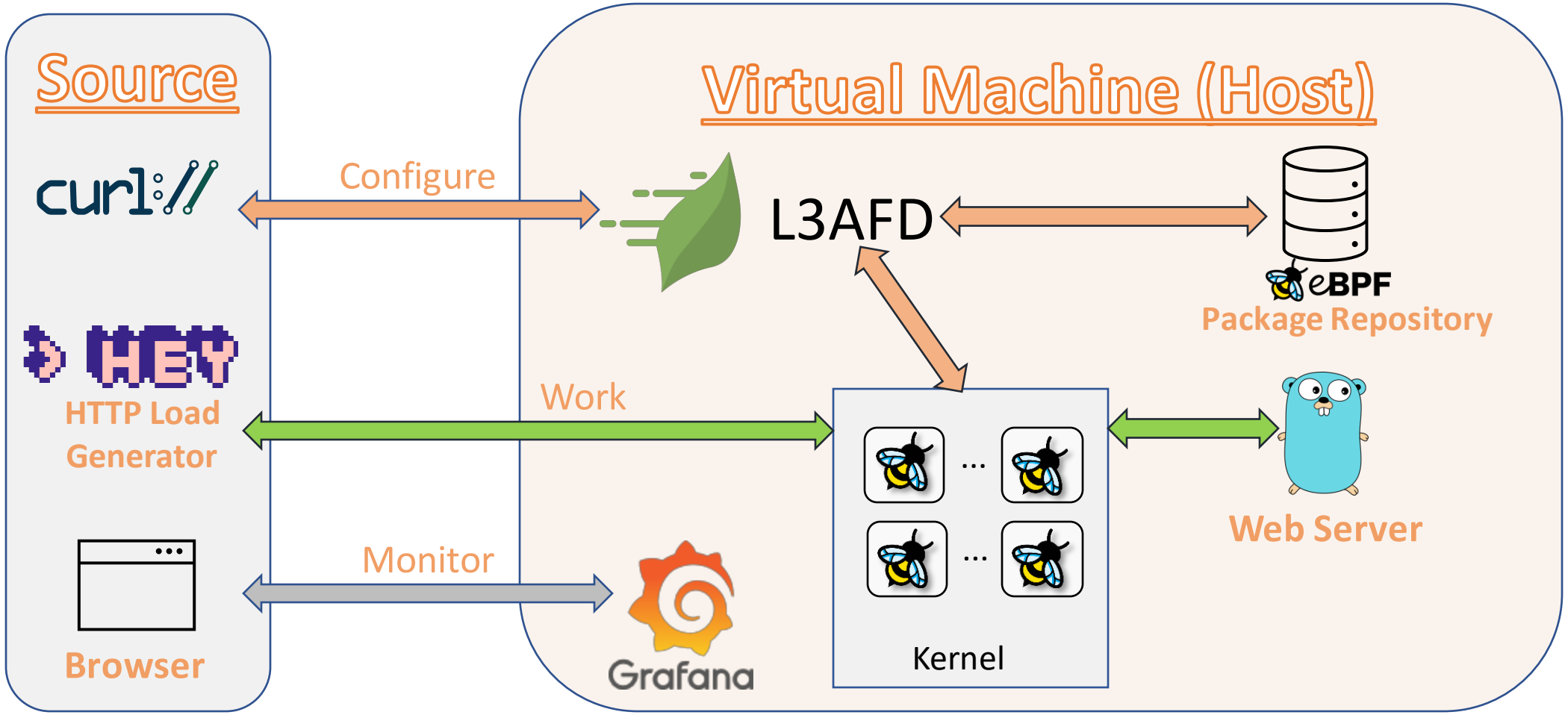
- eBPF-based traffic mirroring solution
- TC hooks are used to examine every incoming/outgoing traffic.
- bpf_clone_redirect BPF helper function Clones ingress/egress traffic and sends it to a remote collector
- Custom filters based on 5 tuple (sa, da, sp, dp, proto)
- Sends mirrored packets to collector on a GUE tunnel
- Trims the packets and mirrors the header data (if required), thereby limiting the bandwidth utilization



https://medium.com/walmartglobaltech/open-sourcing-traffic-mirroring

https://github.com/l3af-project/eBPF-Package-Repository/traffic-mirroring

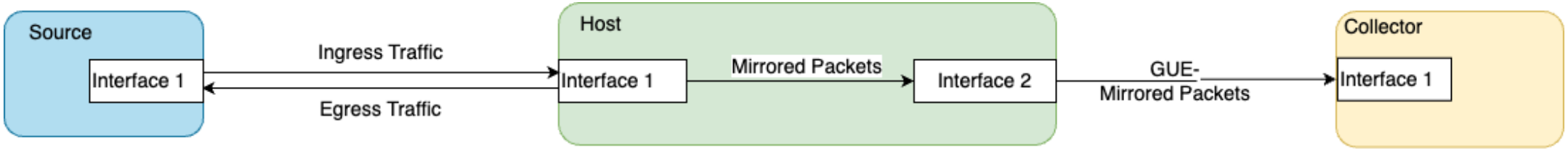
L3AF: Development Environment



https://github.com/l3af-project/l3af-arch/tree/main/dev_environment

TMT: Development Environment

- Vagrant-based TMT development environment
- Creates two VMs
  - Host: Traffic mirroring will be installed
  - Collector: Destination for the mirrored traffic
- We will generate traffic via "hey" tool from the Source machine



TMT: Demo

DEMO

References

https://l3af.io/

https://github.com/l3af-project

https://wiki.lfnetworking.org/display/L3AF/Getting+Started+with+L3AF

Reach us @

Post: main@lists.l3af.io

Slack: https://app.slack.com/client/T02GD9YQJU

Join us @ weekly TSC meeting on Tuesday

When: 15:00 to 16:00 UTC

Where: https://zoom-lfx.platform.linuxfoundation.org/meeting/99638355342?password=c1421101-17dc-4d3d-98cf-3dafdff39057

Q&A

Thank you!