Securing Envoy

Disclaimer & Intro

- We will not cover everything
- DYOR

Best Practices

- Threat model
  - https://www.envoyproxy.io/docs/envoy/v1.15.0/intro/arch_overview/security/threat_model.html
- Configuration recommendation
  - https://www.envoyproxy.io/docs/envoy/v1.15.0/configuration/best_practices/edge
- Will review:
  - Overload manager
  - Admin interface
  - Internal vs External Request
    - More details here: https://www.envoyproxy.io/docs/envoy/v1.15.0/configuration/http/http_conn_man/headers#config-http-conn-man-headers-x-forwarded-for
  - Buffer management
  - Connection Limits

Hardening Tips

- use a minimal image, with no sharp tools (curl, gcc, ssh, etc...)
- envoy doesn’t write files unless you tell it to – set readOnlyRootFilesystem
- remove capabilities
- non root user
- PIE (to allow ASLR)

Stay up to date

- Envoy versions that receive security updates:
  - Envoy master branch (The master branch is considered RC quality)
  - Envoy versions released in the last 12 months
  - See more info here: https://github.com/envoyproxy/envoy/blob/master/RELEASES.md
- Join the announcement mailing list to get notified of pending security updates
  - https://groups.google.com/forum/#!forum/envoy-announce
- Use a vendor that’s on the Private Distributors List (or become an end-user)
  - https://github.com/envoyproxy/envoy/blob/master/SECURITY.md#members

Questions?