solo.io

ambient mesh

What's a Zero-Trust Tunnel?

Exploring Security and Simpler Operations with Istio Ambient Mesh

Jim Barton

Field Engineer - North America @ Solo

@jameshbarton

jim@solo.io

https://www.linkedin.com/in/jameshbarton/

solo.io

Marino Wijay

Platform Advocate - DevRel @ Solo

Organizer - KubeHuddle Toronto

Ambassador - EddieHub Inc.

@virtualized6ix

marino.wijay@solo.io

https://www.twitch.tv/virtualized6ix

https://marinow.hashnode.dev

https://www.linkedin.com/in/mwijay/

#70daysofServiceMesh

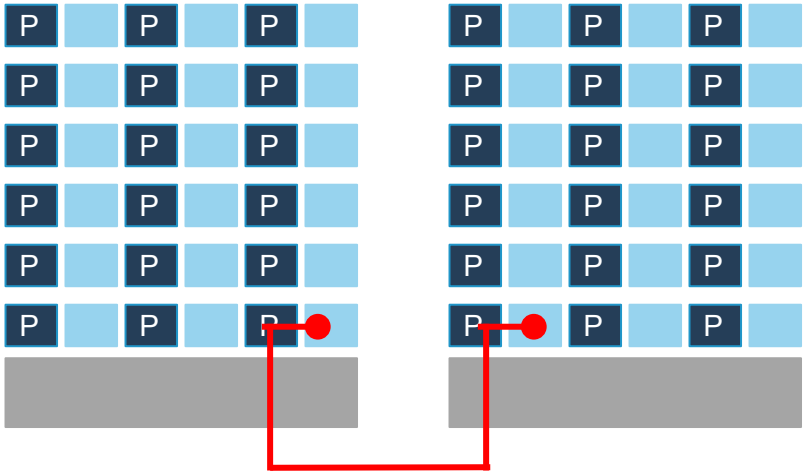
https://linkfree.eddiehub.io/distributethe6ix

solo.io

A 30,000 FT overview of Ambient Mesh

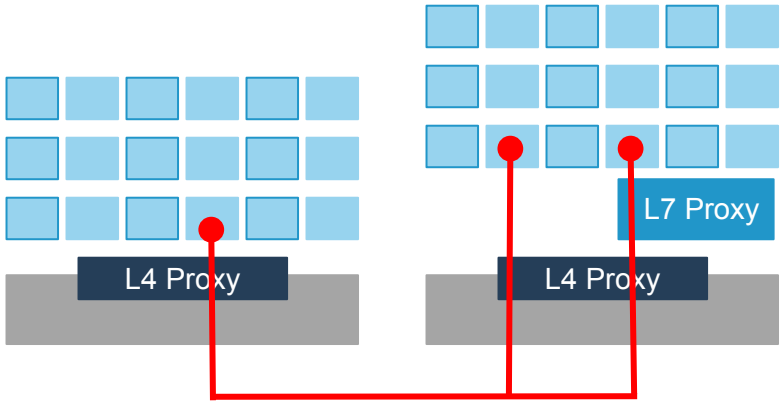
Istio enables Zero-Trust Security

Istio Security with Sidecar Proxy



- All traffic goes through Proxy
- Proxy manages mTLS, Identity
- Proxy manages L7 Application Filters | Policies

Istio Security with Ambient Mesh



- All traffic goes through Proxy
- L4 Proxy manages mTLS, Identity
- L7 Proxy manages L7 Application Filters | Policies

Introducing Istio Ambient Mesh

ambient mesh

Reduce Costs

- Proxy per Node
- Multi-Tenant Proxy
- Lightweight (L4) Proxy implementation (uProxy)

Simplify Operations

- Mesh is Transparent to Applications
- Decouple Proxy from Applications
- Simplify Adding new Apps
- Simplify App Updates

Improve Performance

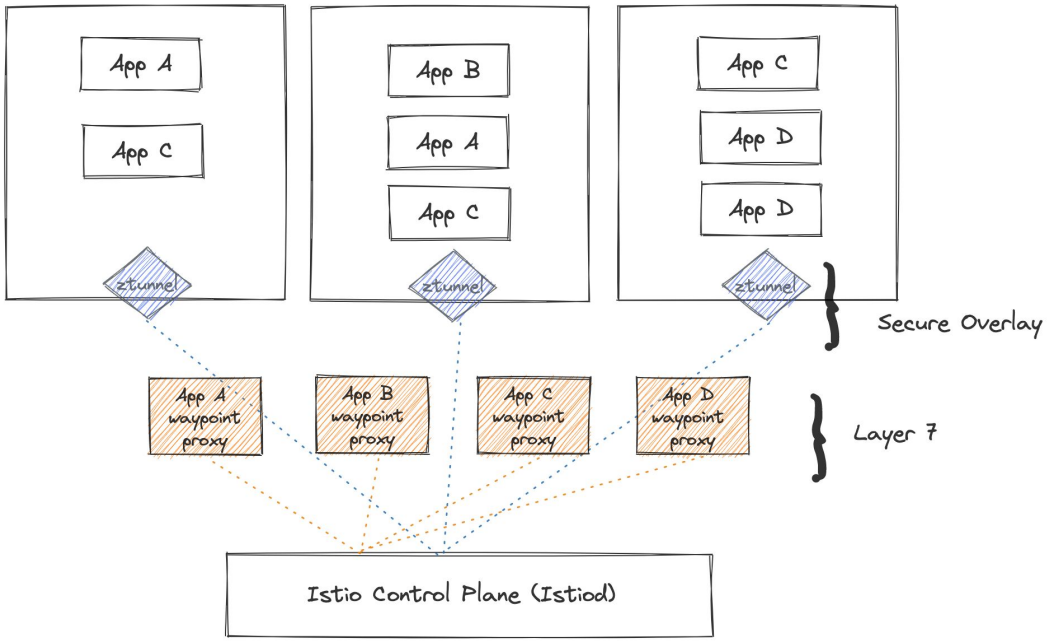
- uProxy is L4 vs L7
- uProxy can use acceleration in OS (eBPF)

Zero Trust Security

solo.io

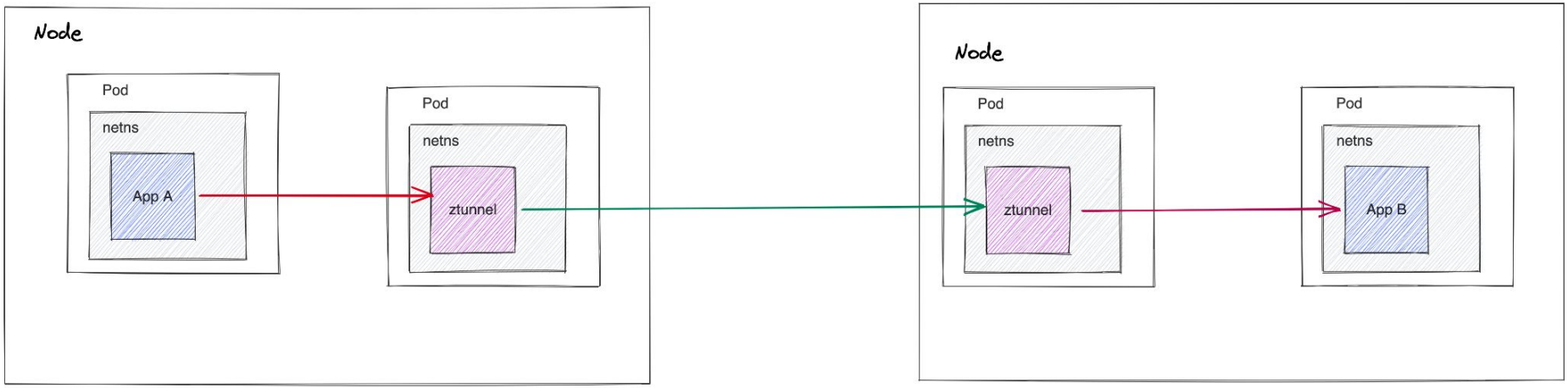
How does Istio ambient work?

- Separate mesh capabilities into L4 and L7
- Adopt only the capabilities you need
- Remove the data plane from the workload (no sidecar)
- Leverage more capabilities in the CNI
- Reduce attack surface of data plane



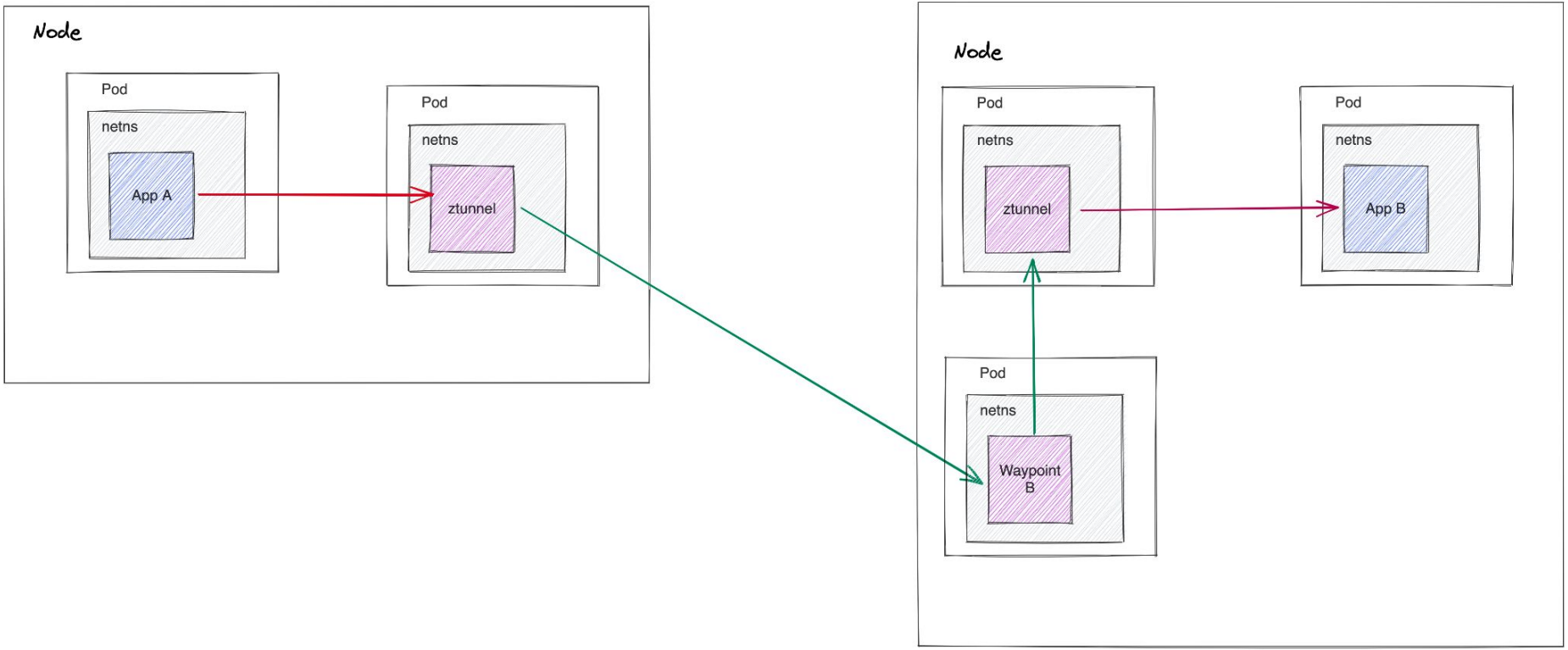
solo.io

How does it work (secure overlay only)?



solo.io

How does it work (secure overlay + L7)?



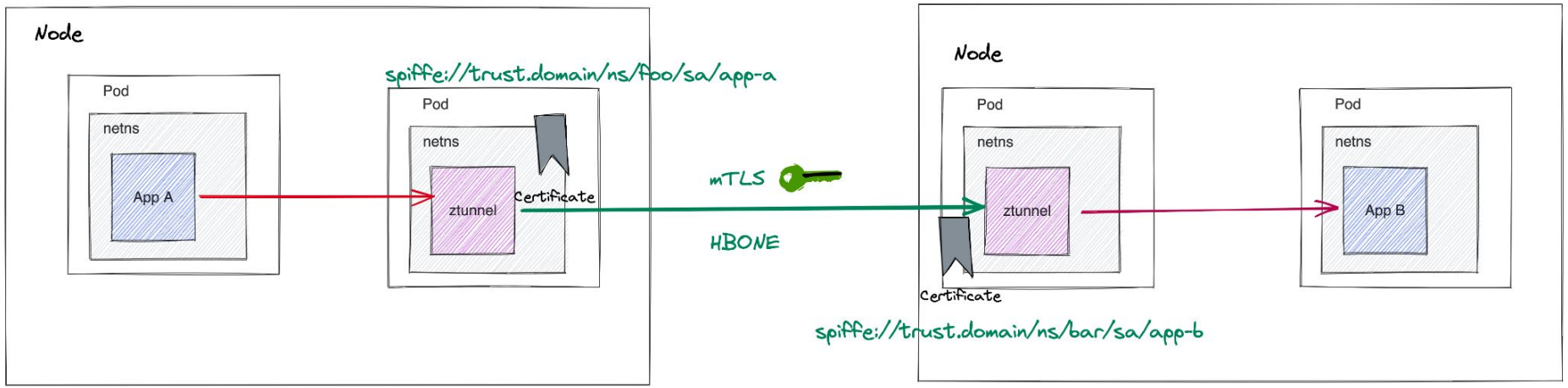
solo.io

Benefits

- No more race conditions between workload containers and sidecar/init-container, etc
- Don’t need to inject Pods / alter deployment resources
- Upgrades are out of band / transparent from the application
- Limited risk profile for opting into mesh features
- Reduced blast radius of application vulnerabilities
- Reduced blast radius of application vulnerabilities
- Cost savings with reduced data plane components
- Maintain isolated tenancy, customization, configuration
- Maintain the foundations of zero-trust network security
- Improved performance

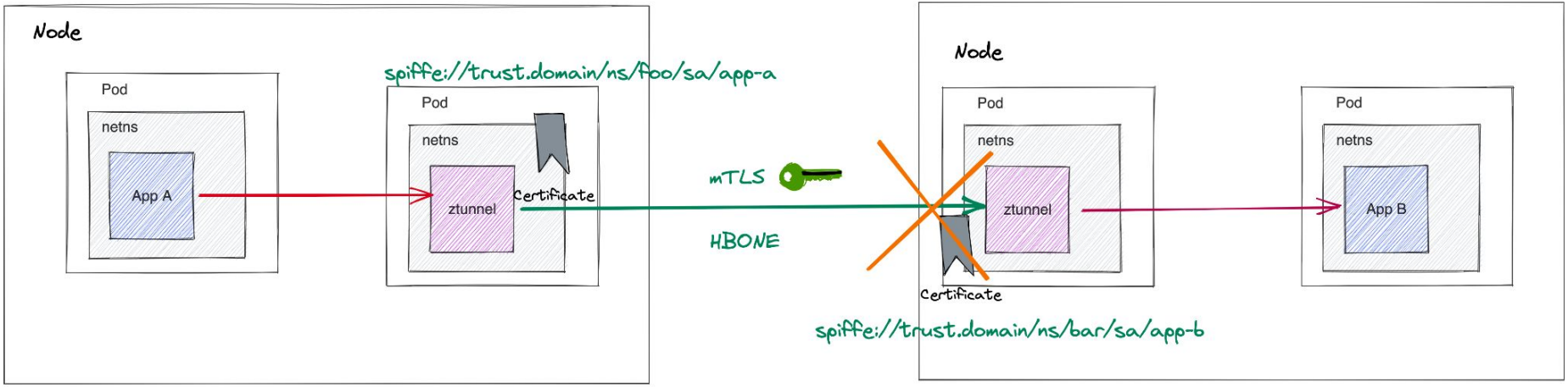
Taking a closer look at Istio Ambient secure-overlay layer

mTLS with Istio Ambient



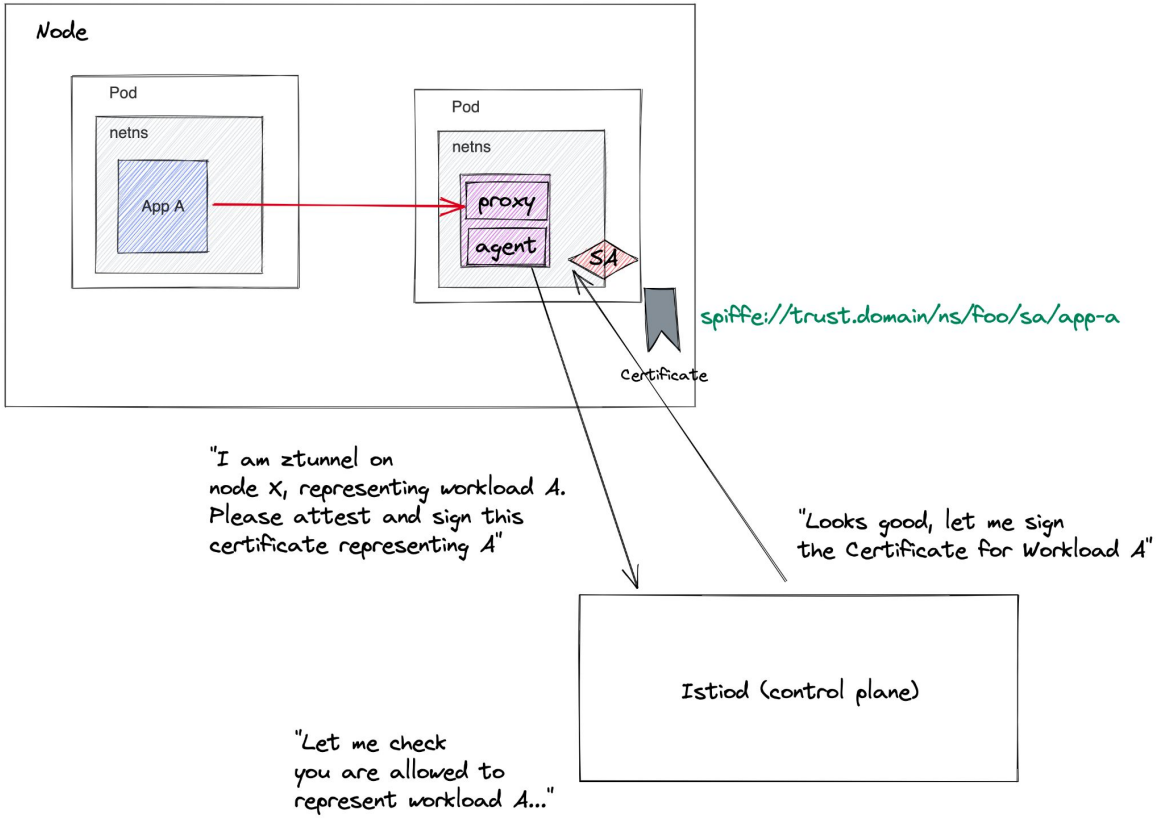
solo.io

Authorization Policy with Istio Ambient



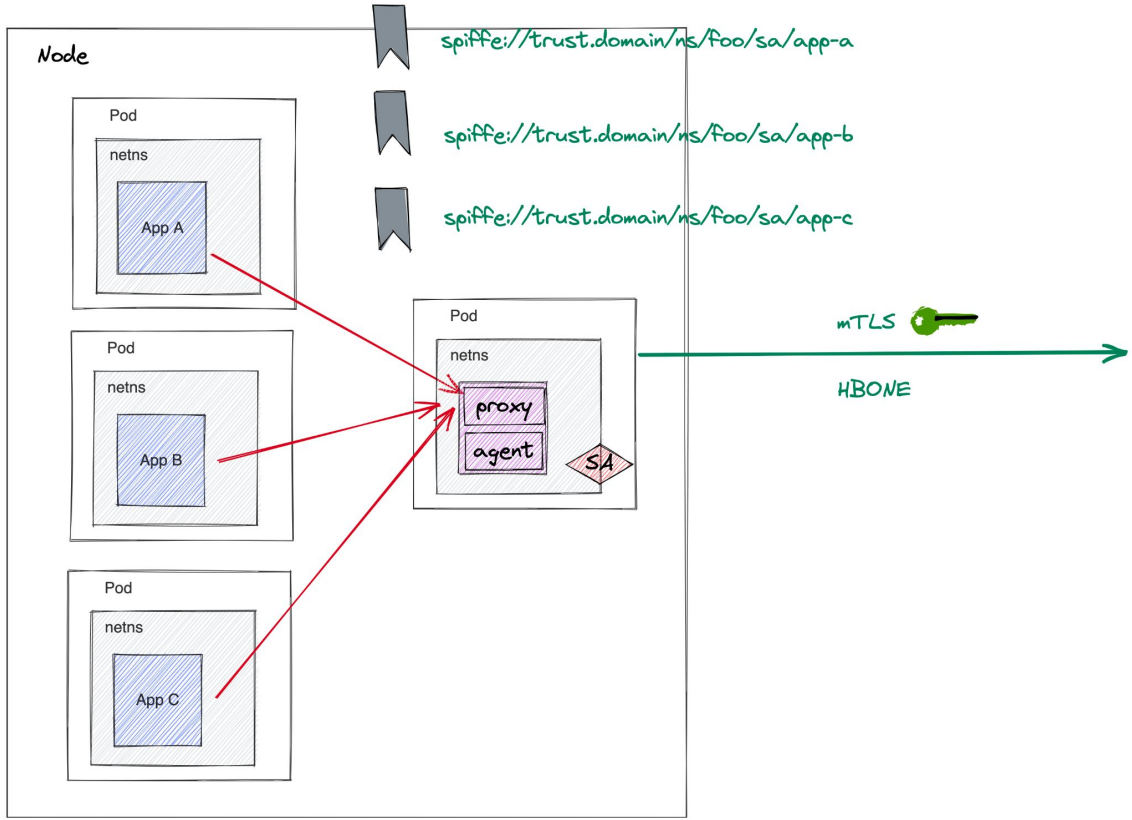
solo.io

How ztunnel gets certificates



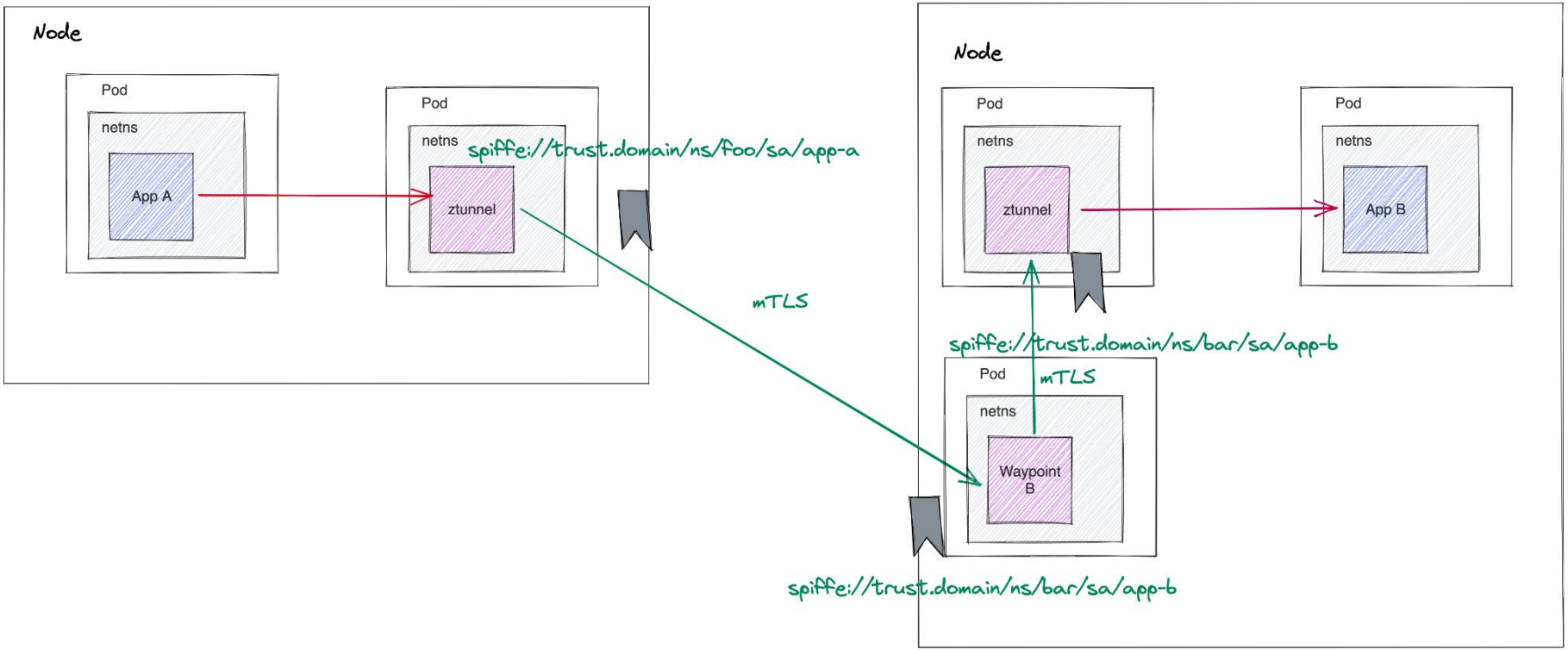
solo.io

How ztunnel gets certificates



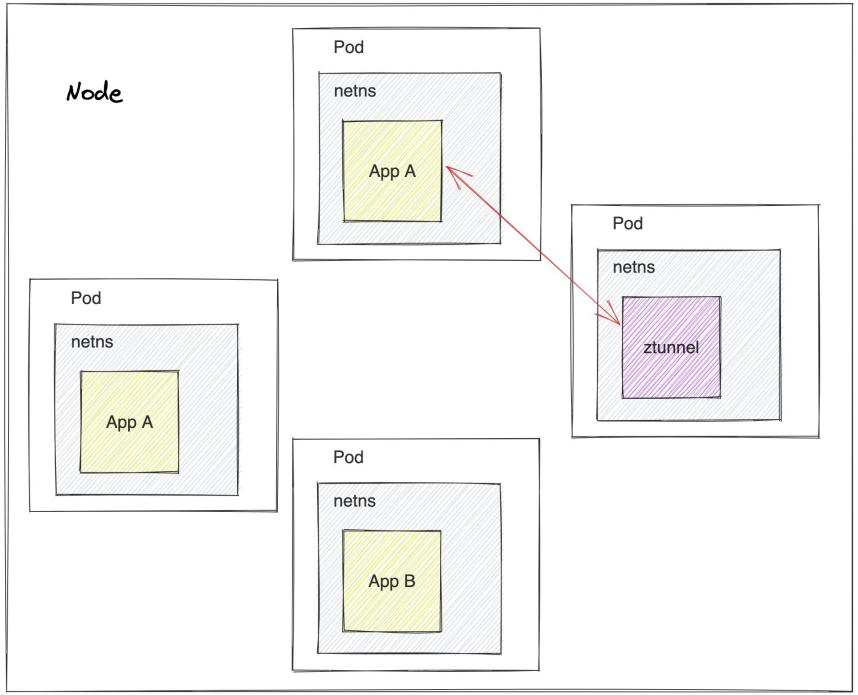
solo.io

How communication is secured through waypoint proxy



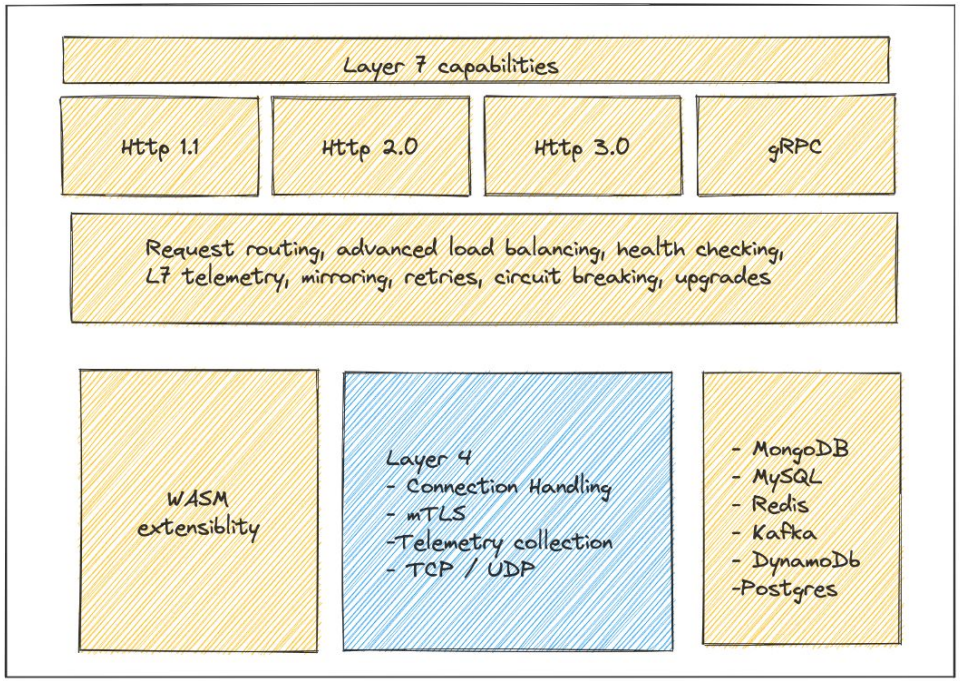
solo.io

App compromise (ambient)

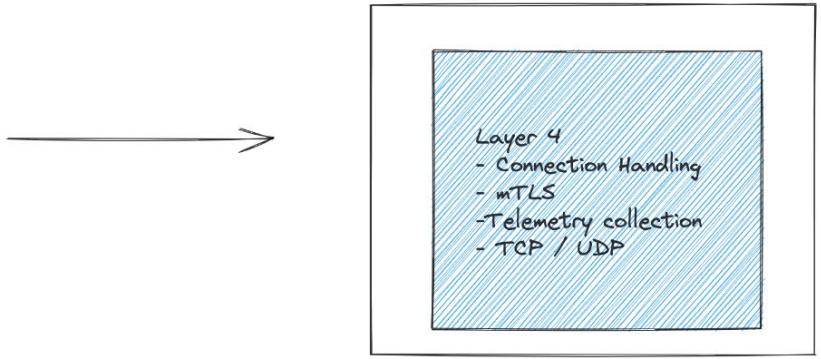


solo.io

Smaller exposure for secure overlay/ztunnel



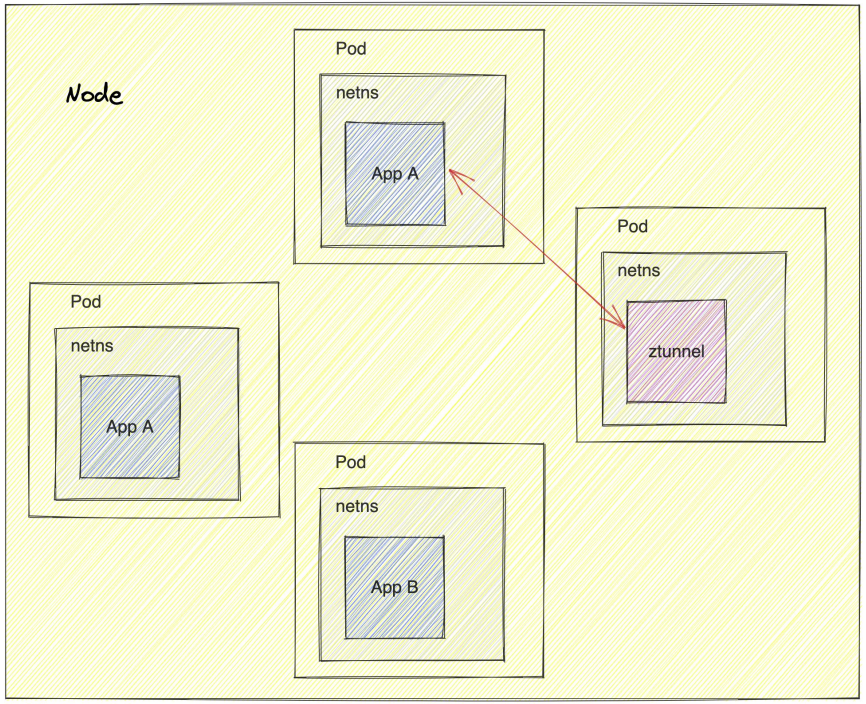
Fully blown Policy Enforcement Point (L7) Proxy



ztunnel

solo.io

Node compromise (ambient)



solo.io

Istio Ambient Mesh Demonstration

ambient mesh

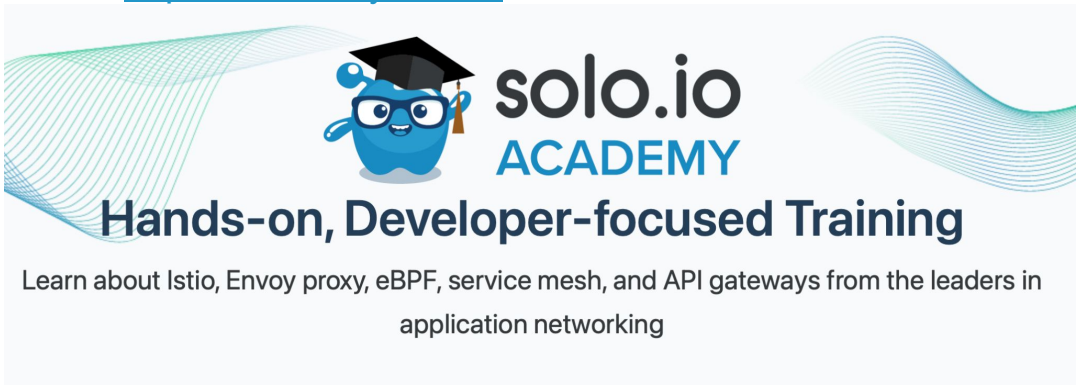
solo.io

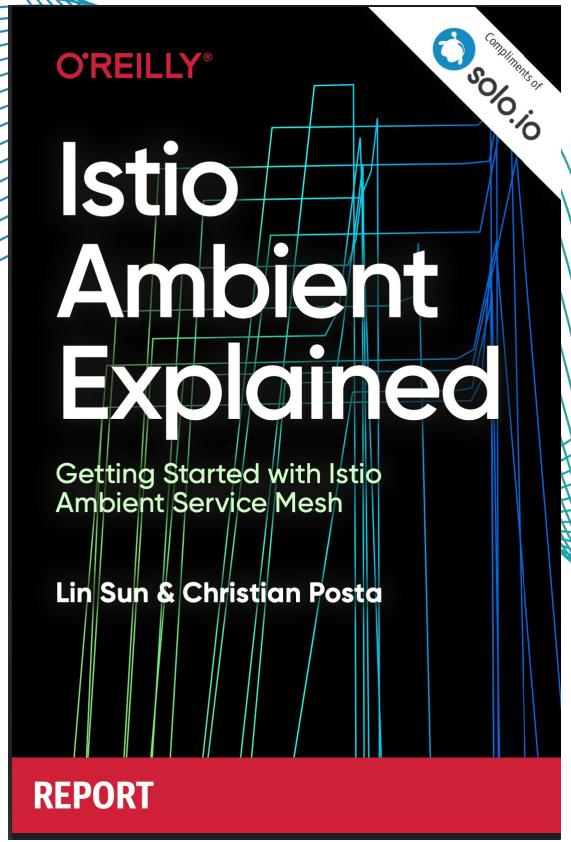
Recap

- Data plane deployment topology differs from Sidecar
- Improvement in security posture by separating data plane component from applications
- Ambient reduces attack surface of data plane running on node with workloads for secure-overlay layer
- Ztunnel component needs to be treated similarly as any other shared-node component (CNI, kubelet, etc)
- Operational improvements to Istio greatly improve CVE patching strategy

Want to learn more?

- Download the Free Ambient Book
  http://bit.ly/ambient-book
- Come visit Solo.io at Booth G18 in the Exhibit Hall
- Free hands-on workshops:
  https://academy.solo.io





solo.io

Thank You!