

Using Istio to Build the Next 5G Platform

David Lenrow

Open Source Service Mesh Evangelist

Neeraj Poddar

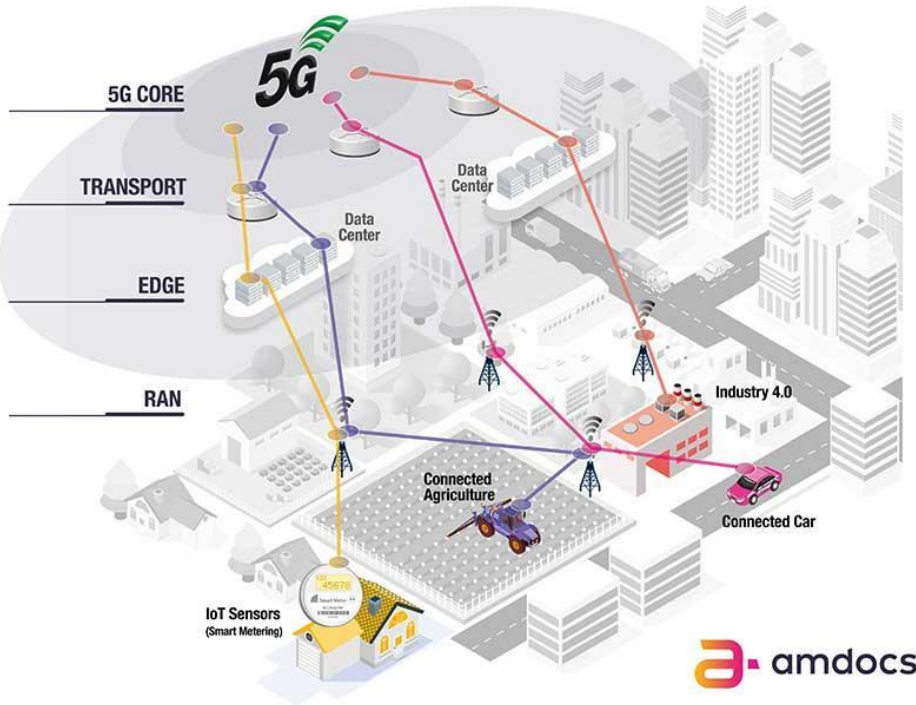
Co-founder & Chief Architect, Aspen Mesh

February 22, 2021

What Is 5G and Why Does It Matter?

End to end lifecycle automation for cross-domain, multi-vendor network slicing

Amdocs 5G Slice Manager - Slice Design - Slice Automation - Slice Operation & Management

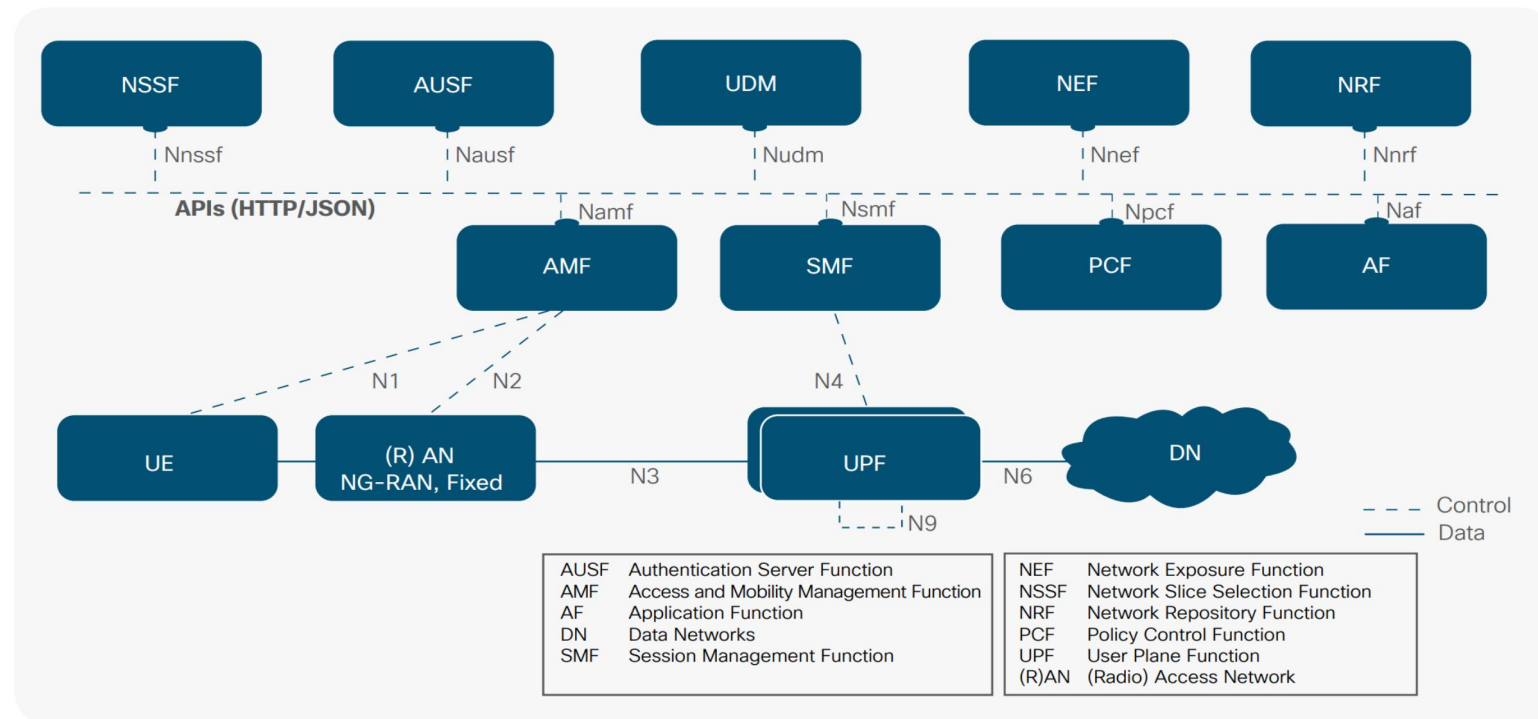


5G wireless technology is meant to deliver higher multi-Gbps peak data speeds, **ultra low latency**, more reliability, massive network capacity, increased availability, and a more uniform user experience to more users.

Higher performance and improved efficiency empower new user experiences and connects new industries.

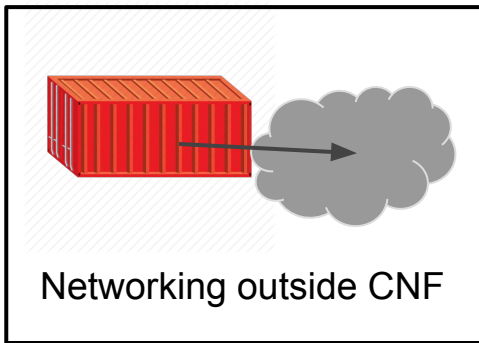
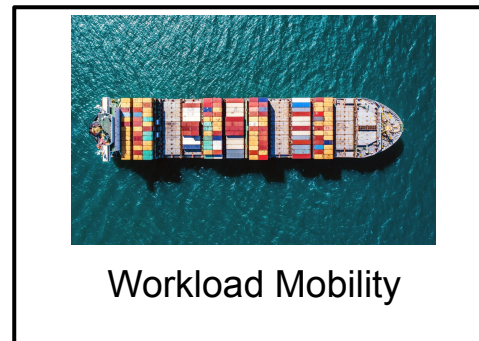
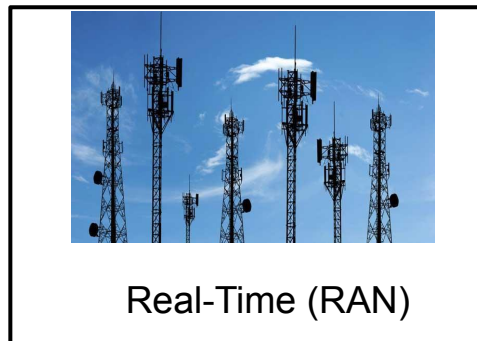
-Qualcomm

5G Architecture



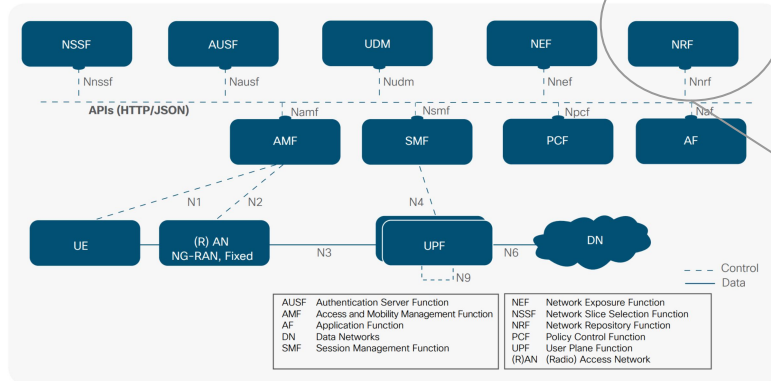
<https://medium.com/5g-nr/5g-service-based-architecture-sba-47900b0ded0a>

Key Platform Requirements

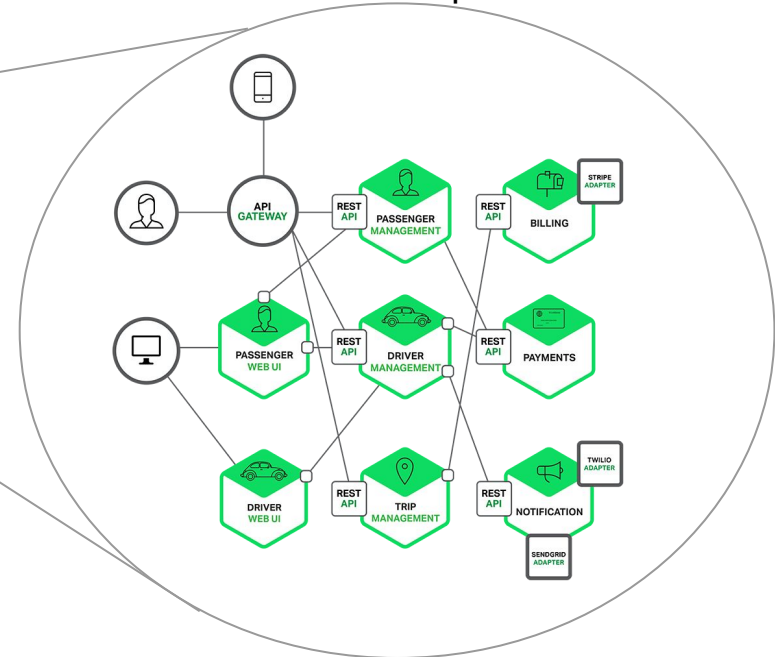


5G Architecture Looks a Lot Like a Mesh?

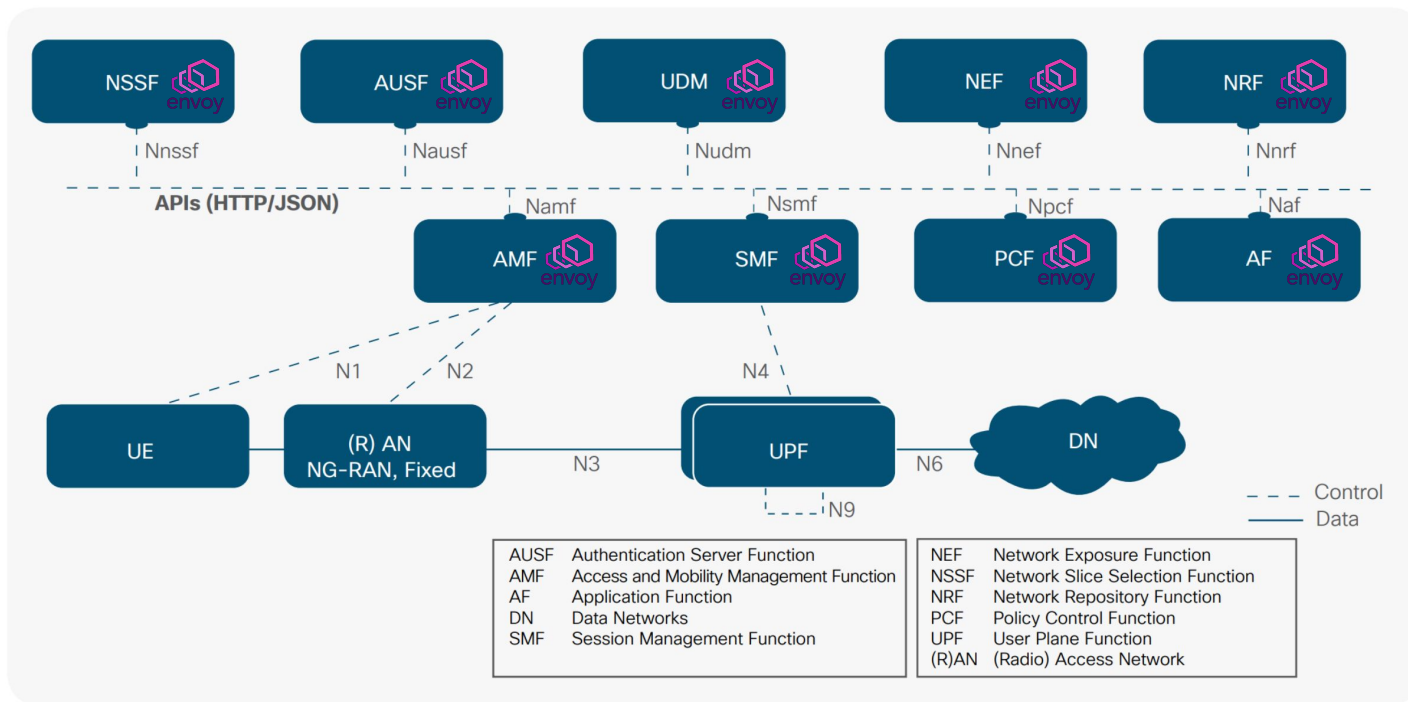
5G Network Function Decomposition



Microservice Network Function Implementation



5G Architecture with Istio



<https://medium.com/5g-nr/5g-service-based-architecture-sba-47900b0ded0a>

What Do You Get From Istio?

Enforcement Primitives to Build Zero Trust

Strong identity for users, workloads, devices, etc.

Encrypting inter-CNF traffic via mutual TLS (mTLS)

Option to encrypt intra-CNF traffic via mTLS

Autonomous PKI service for certificate lifecycle management at scale

Visibility, Observability, Debugging

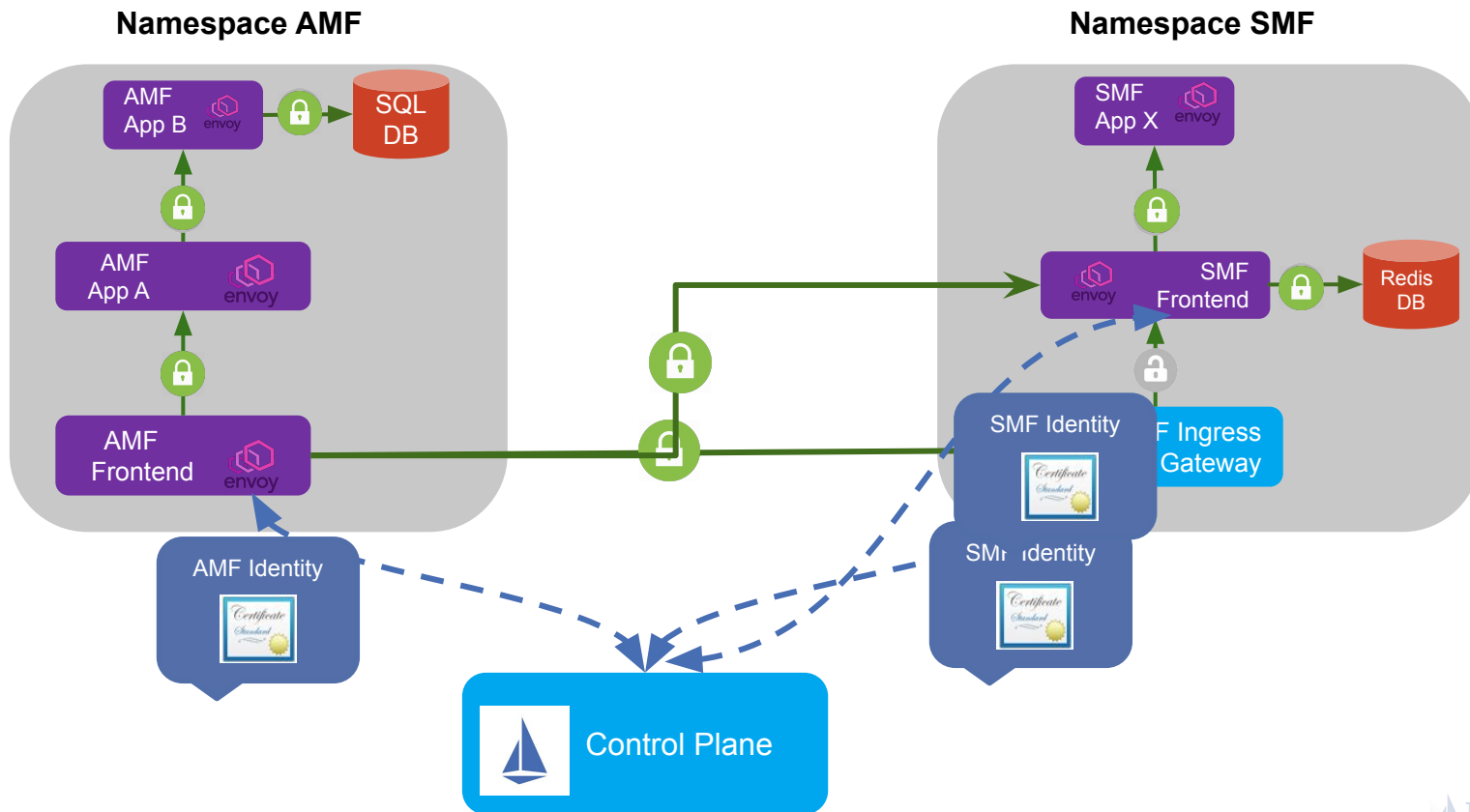
Uniform metrics and tracing for all CNF traffic

Traffic Management

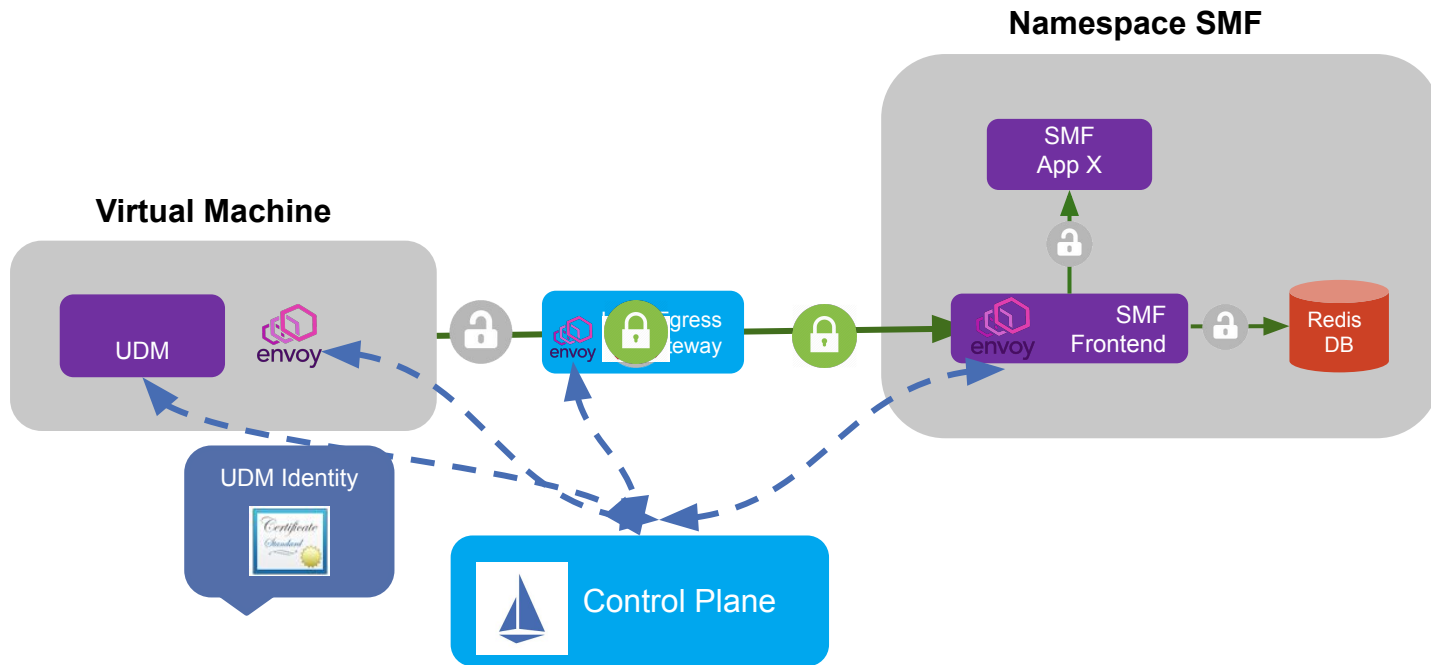
Powerful Layer 7 (HTTP/2) routing

Architecture Options

Namespace Level Tenancy



How to Make Legacy NFs Talk to CNFs in the Mesh



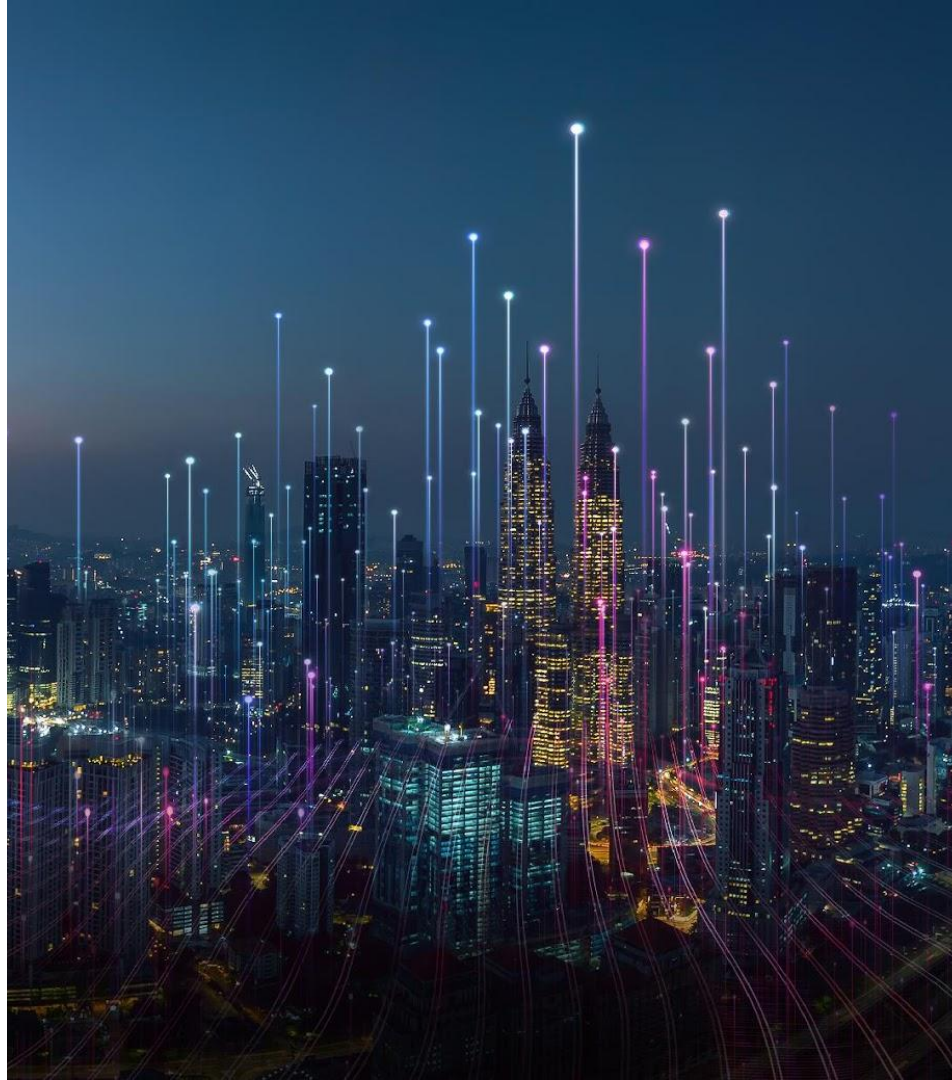
Tuning Istio to Meet 5G Security Requirements

- CNI to avoid escalated pod privileges
- Integrate with PKI minted Intermediate [CA](#)
- Enable ECC certificates
- Configure workload certificate TTLs
- Enable strict mutual TLS (mTLS) instead of auto
- Use dedicated egress gateways



Tuning Istio to Meet 5G Requirements

- Augment tracing to surface 5G specific tags
- Optimize HTTP/2 stream and connection settings
- Configure sidecar proxy concurrency



Learnings Along the Way

- Istio architectural changes
- SPIFFE only certificates
- Configuring workload certificate TTLs
- RSA to ECC migration
- Missing www-authenticate header
- Tuning per-workload proxy concurrency
- Consuming Istio generated certificates at gateways

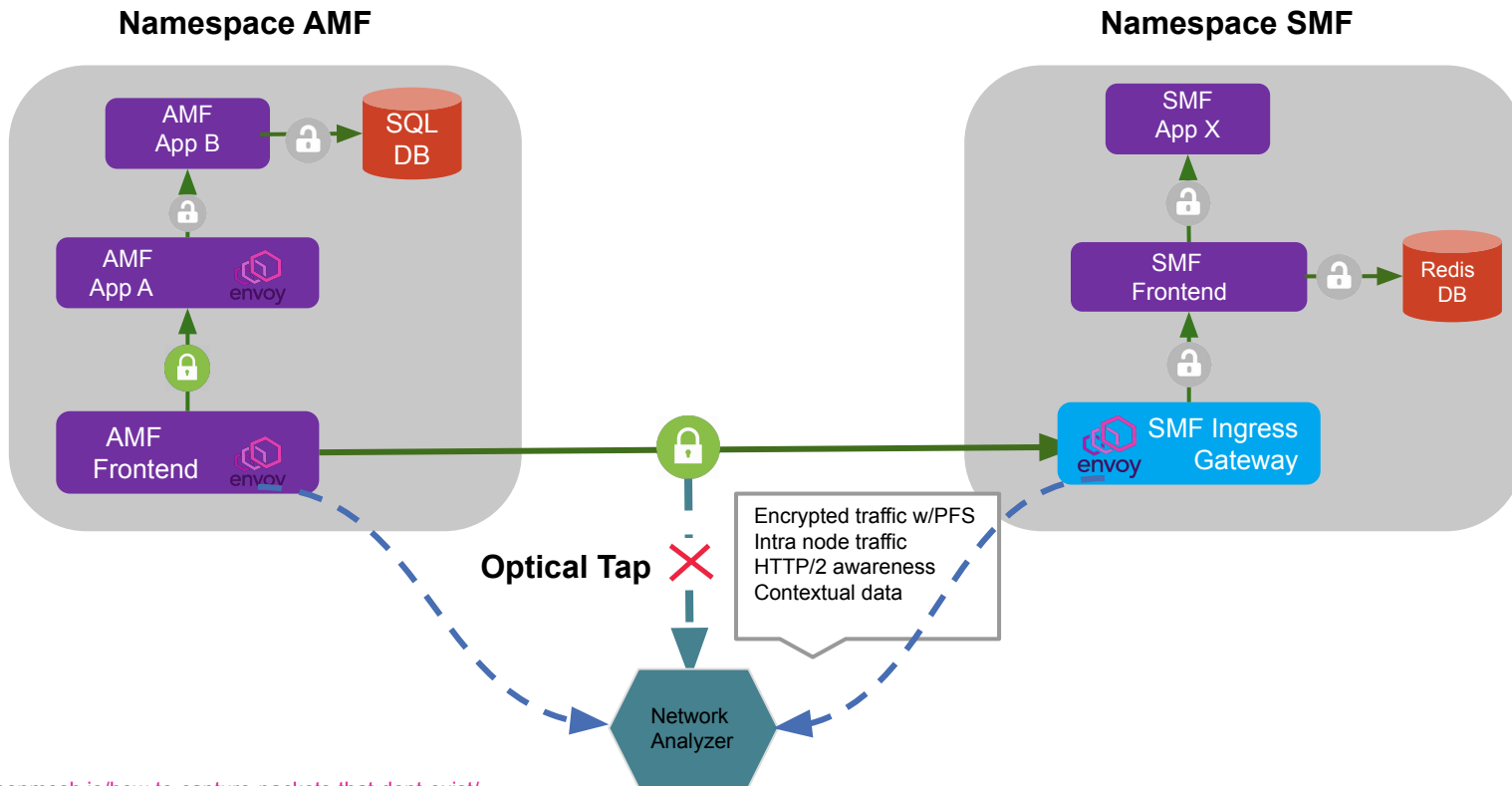


Going Beyond Istio

- 4G to 5G translation (Protocols like Diameter, SCTP, GTP)
- High speed data path (SR-IOV/DPDK)
- Customizing workload certificate attributes
- Multi-cluster/site visibility
- Deep packet inspection



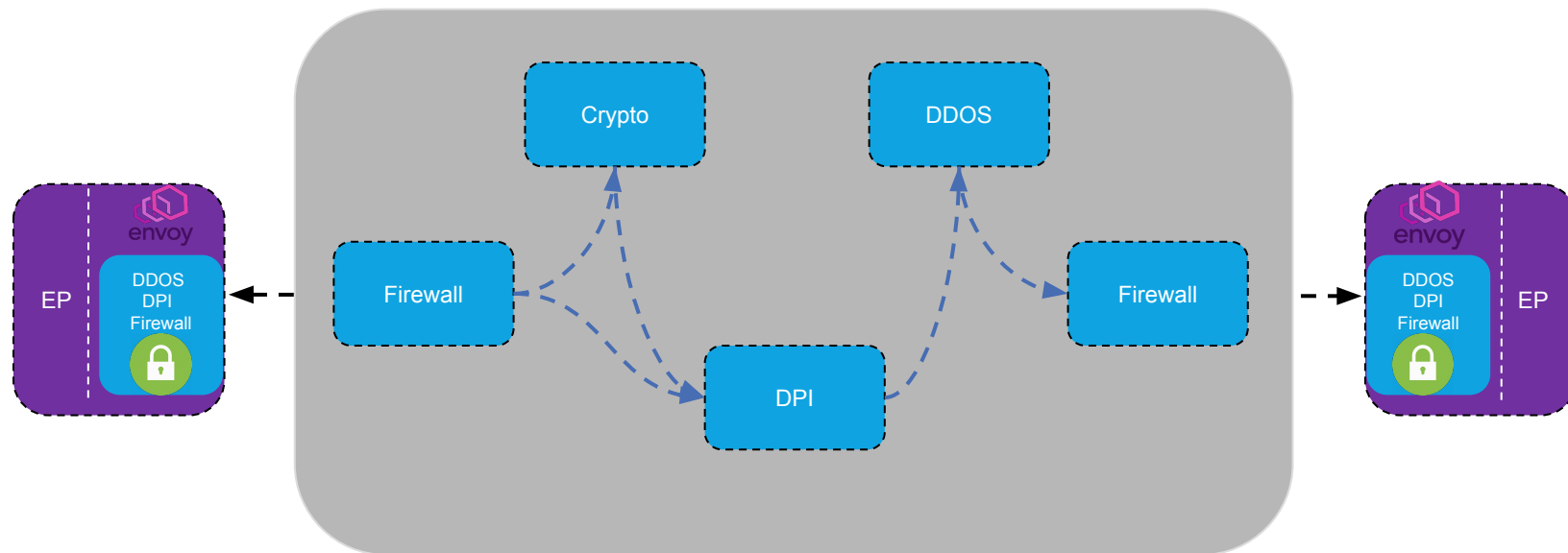
Deep Packet Inspection



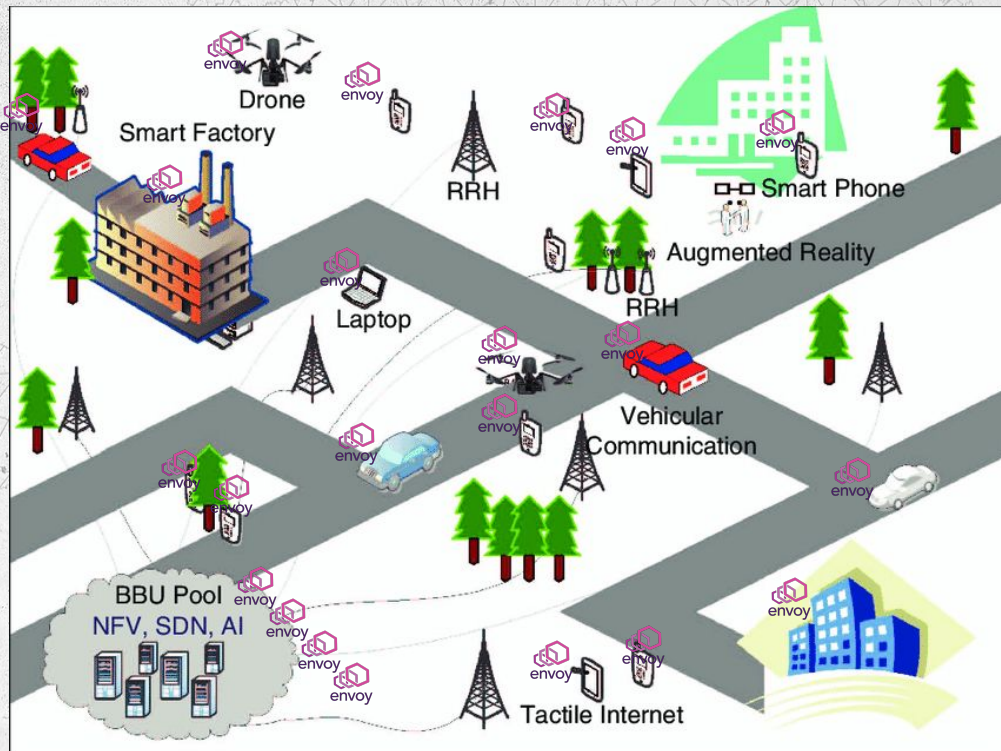
<https://aspenmesh.io/how-to-capture-packets-that-dont-exist/>

Network Architecture

Middleboxes in Network Demarc



Service Mesh Everywhere World!



Thank You!

@nrjpoddar

aspenmesh.io

@dlenrow

IstioCon