

Network Service Mesh in a Nutshell

CNCF Meetup, Sofia

Nikolay Nikolaev
Senior Open Source Engineer, VMware

03/28/2019

Workload management technology evolution

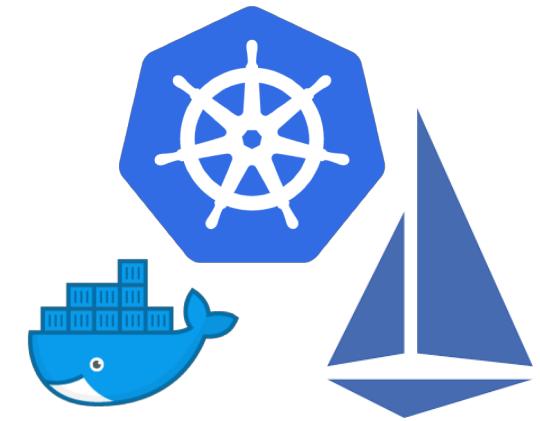
How things changed



Baremetal



Virtual Machines

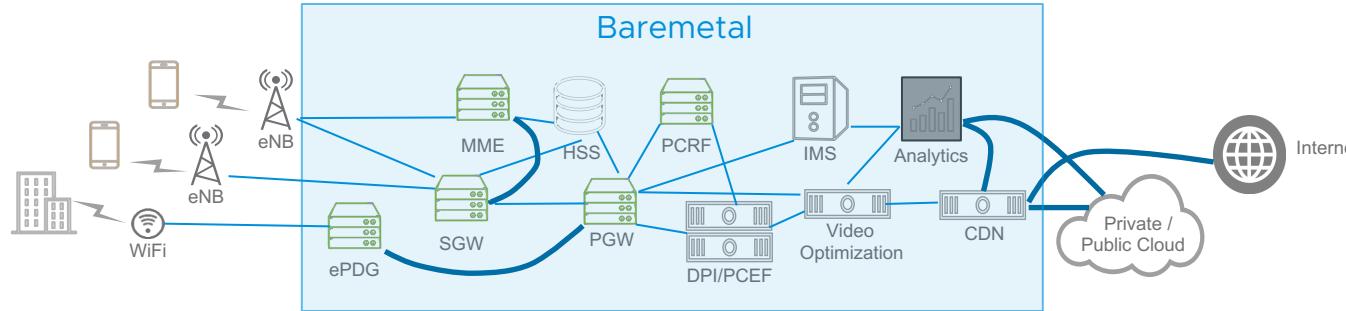


Containers

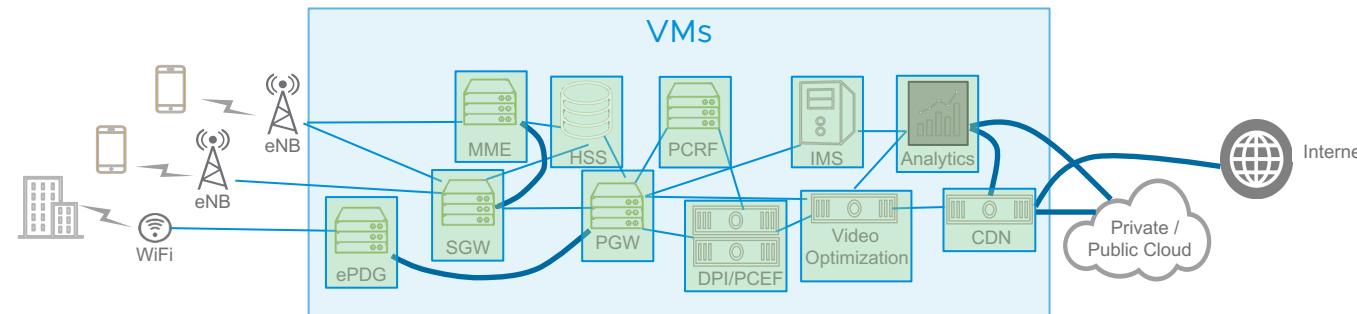
Evolution through the eyes of a telco

Networking Function Virtualization (NFV)

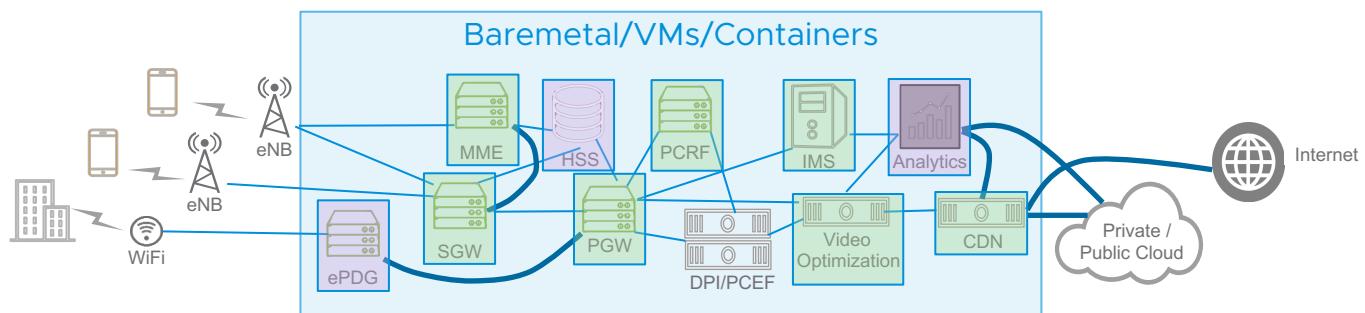
10 years ago



Today



What's next?



Telco benefits of adopting the “container” approach

Defining the next NFV

- Containerize workloads
- Orchestration by Kubernetes
- Heterogenous workload deployment
- Leverage the benefits of Service Mesh

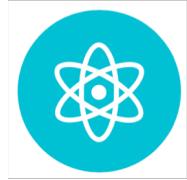
What is Service Mesh?

Service Mesh is ...



Discoverable

Services can find each other.



Resilient

Built-in robustness frameworks, load balancing & test infrastructure.



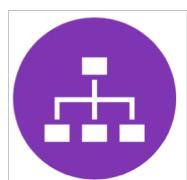
Configurable

Configure services dynamically at runtime.



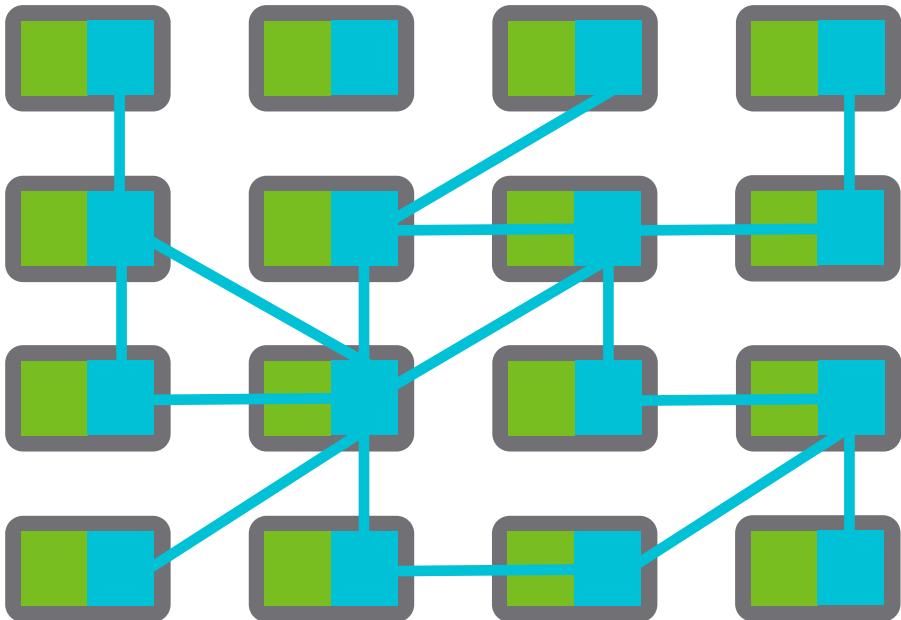
Observable

Standardized metrics, logging, monitoring & distributed tracing.



Secure

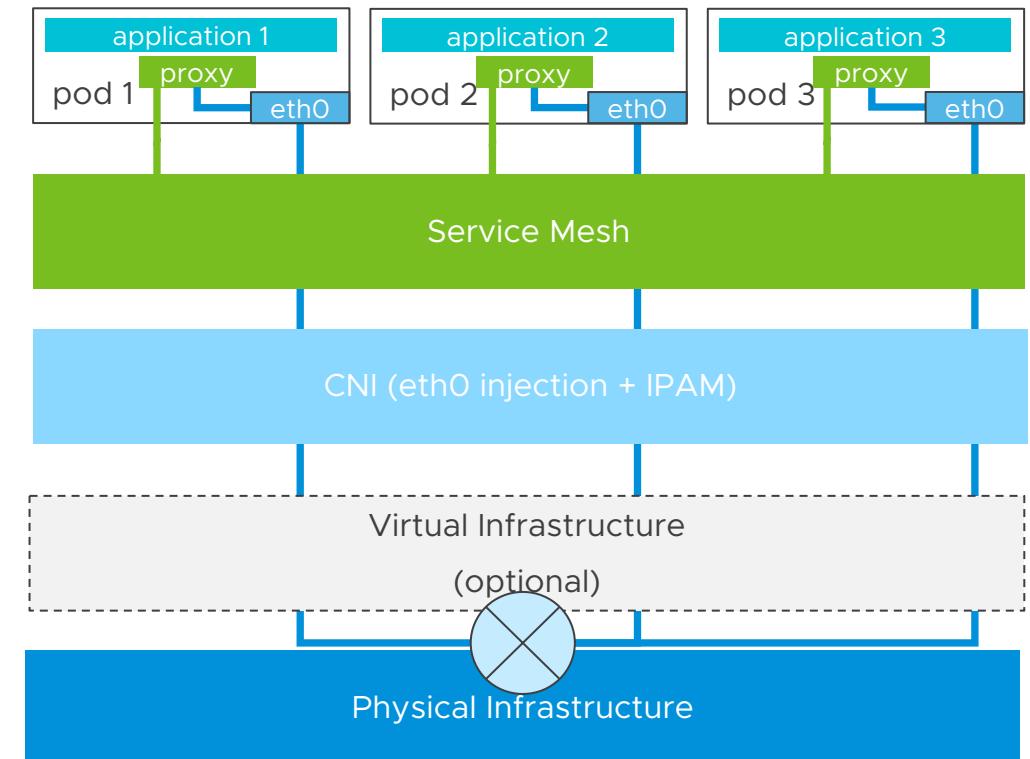
Encrypt and protect service communication.



What happens under the hood?

A simple Service Mesh example

- Applications are deployed as Kubernetes Services
- The Service Mesh injects its proxies
- Intercepts Ingress/Egress traffic
- Monitoring/traceability
- Resiliency
- Security



What's missing?

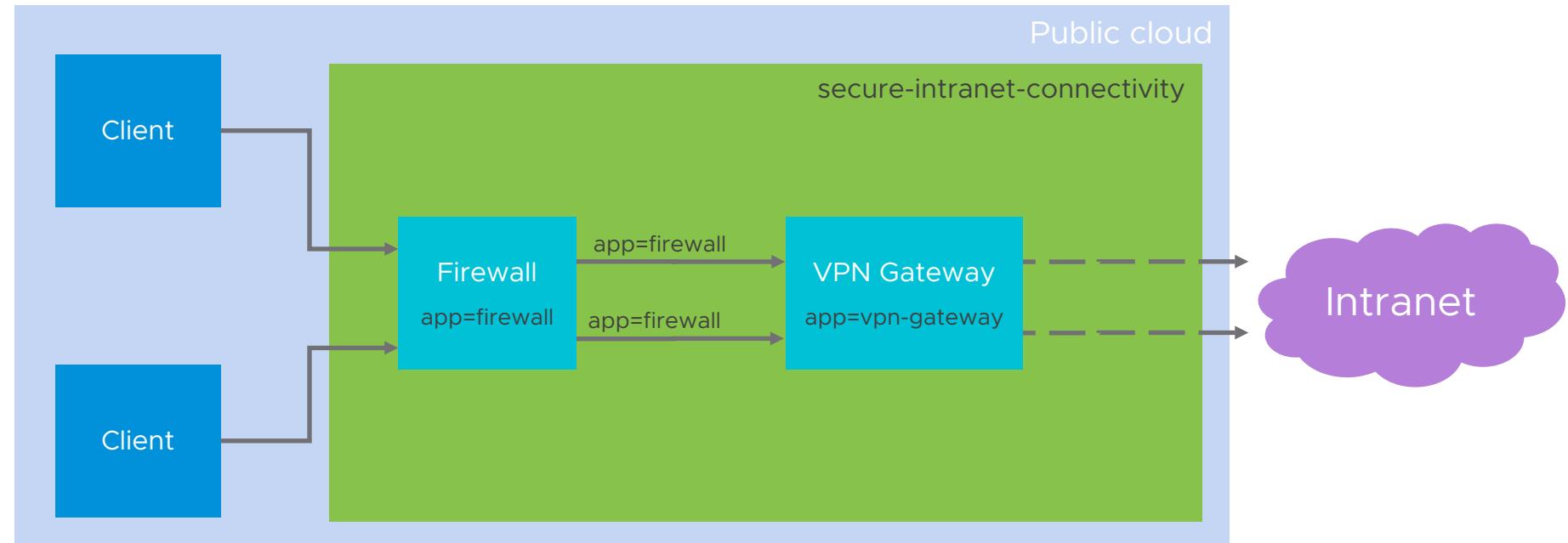
- Traditional Service Mesh implementations focus mostly on L4-L7
- Network Service Mesh (NSM) covers typically L2/L3, but can be virtually “anything”

Layer	OSI	TCP/IP	Service Mesh
7	Application		
6	Presentation	HTTP/HTTP2	Istio
5	Session		
4	Transport	UDP, TCP	Istio
3	Network	IP	NSM
2	Data link	Ethernet	NSM
1	Physical	Copper/Fiber Wireless	NSM*

Introduction to Network Service Mesh

What is a Network Service?

- A client running in the public cloud needs a connection to the Corporate Intranet
- Deploy the Network Service and Endpoints
- A client requests the secure-intranet-connectivity



Describing a Network Service

Service definition in Network Service Mesh

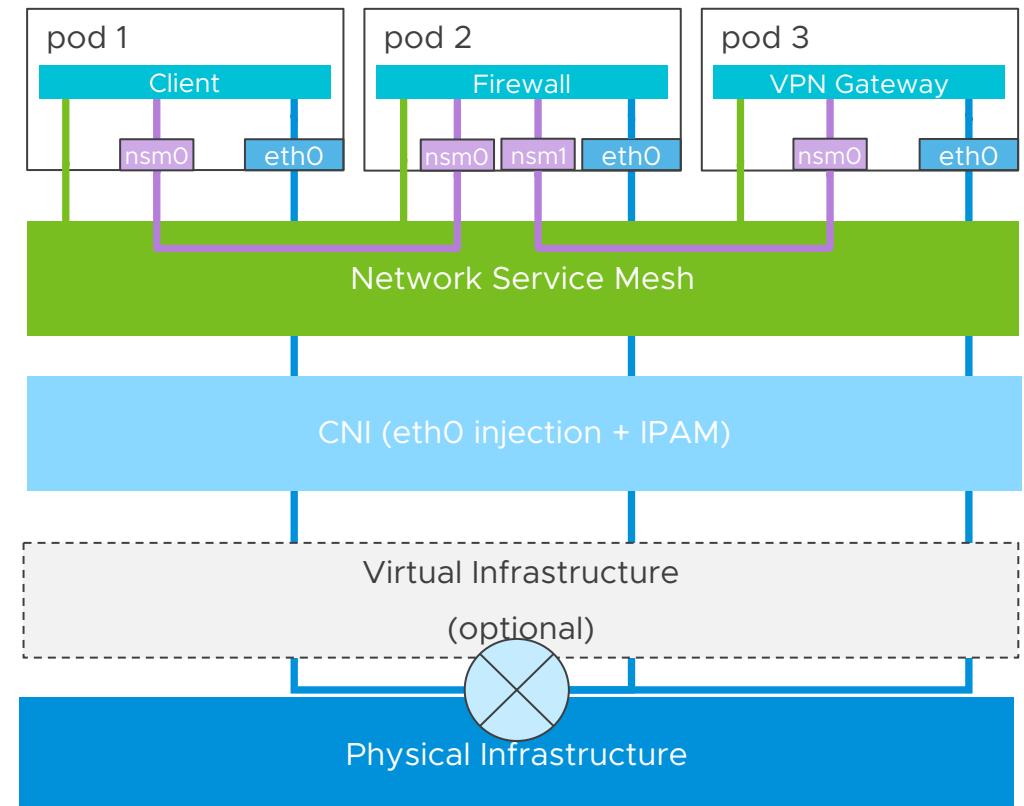
- Source and destination selection
- Service composition
- Endpoint implementation

```
apiVersion: network servicemesh.io/v1
kind: NetworkService
metadata:
  name: secure-intranet-connectivity
spec:
  payload: IP
  matches:
    - match:
        sourceSelector:
          app: firewall
        route:
          - destination:
              destinationSelector:
                app: vpn-gateway
    - match:
        route:
          - destination:
              destinationSelector:
                app: firewall
```

What happens under the hood?

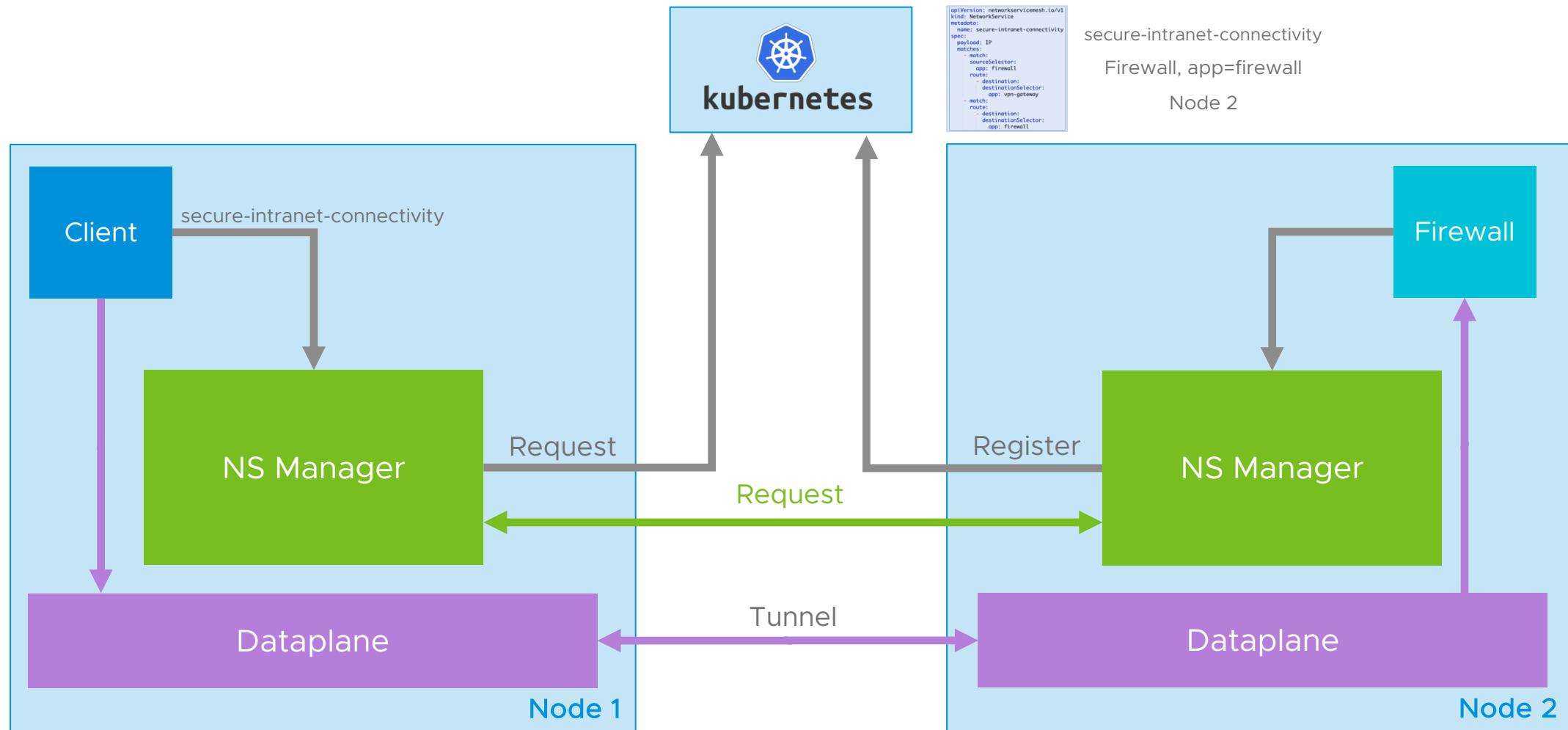
A simple Network Service Mesh example

- The default CNI (eth0) network is used for Kubernetes management (livecheck, etc)
- The Endpoints are announced to NSM
- The Client asks for the Network Service
- The full NS mesh is build



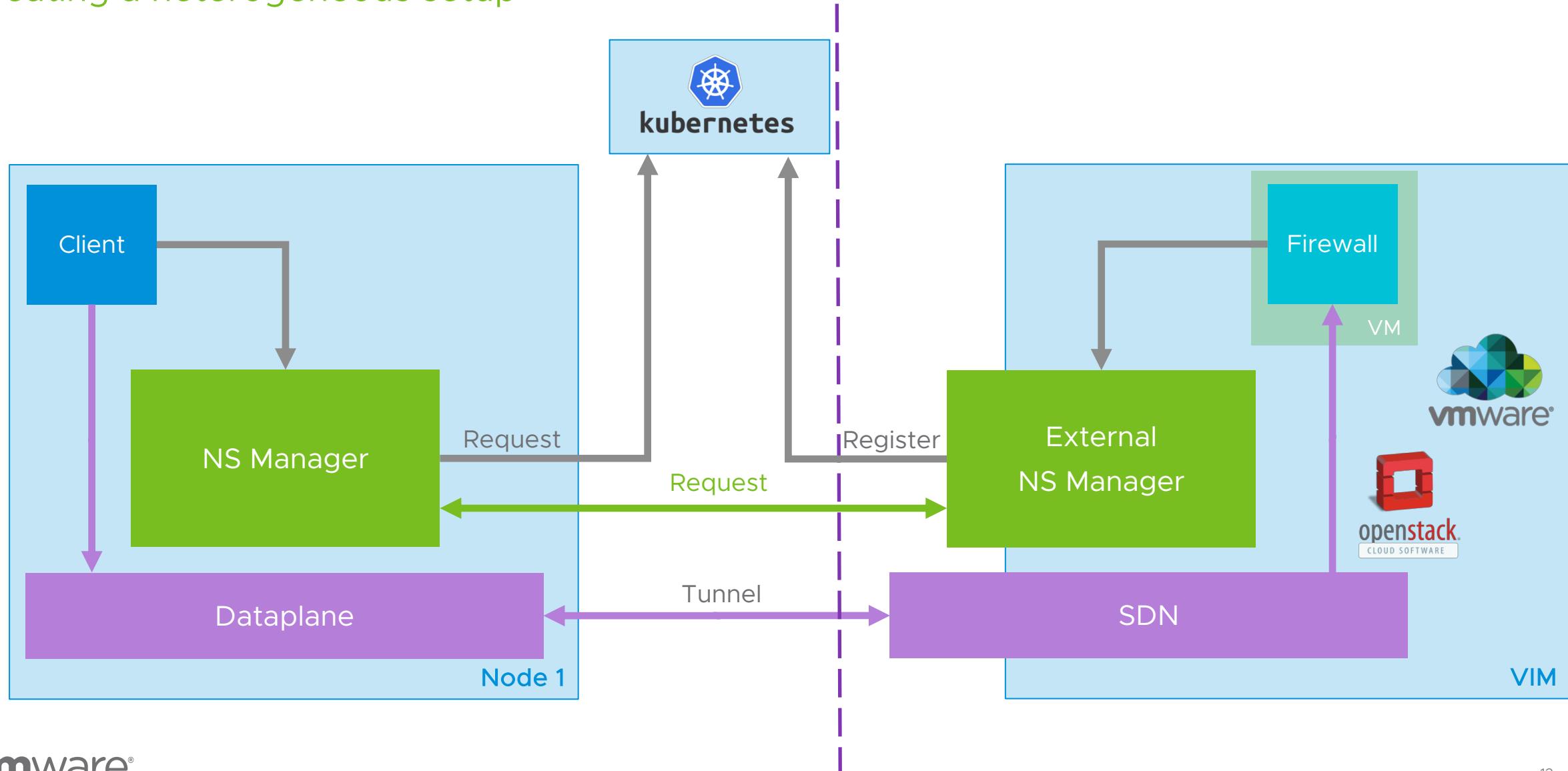
How it works?

Multi node setup with Kubernetes



Extending the concept

Creating a heterogeneous setup



Network Service Mesh use cases

- Telco setups
 - NFV, Edge, 5G
- Enterprise networking
 - CNI
 - Traditional Service Mesh
- Storage
 - SAN
- HPC
 - Infiniband, RDMA

What's next?

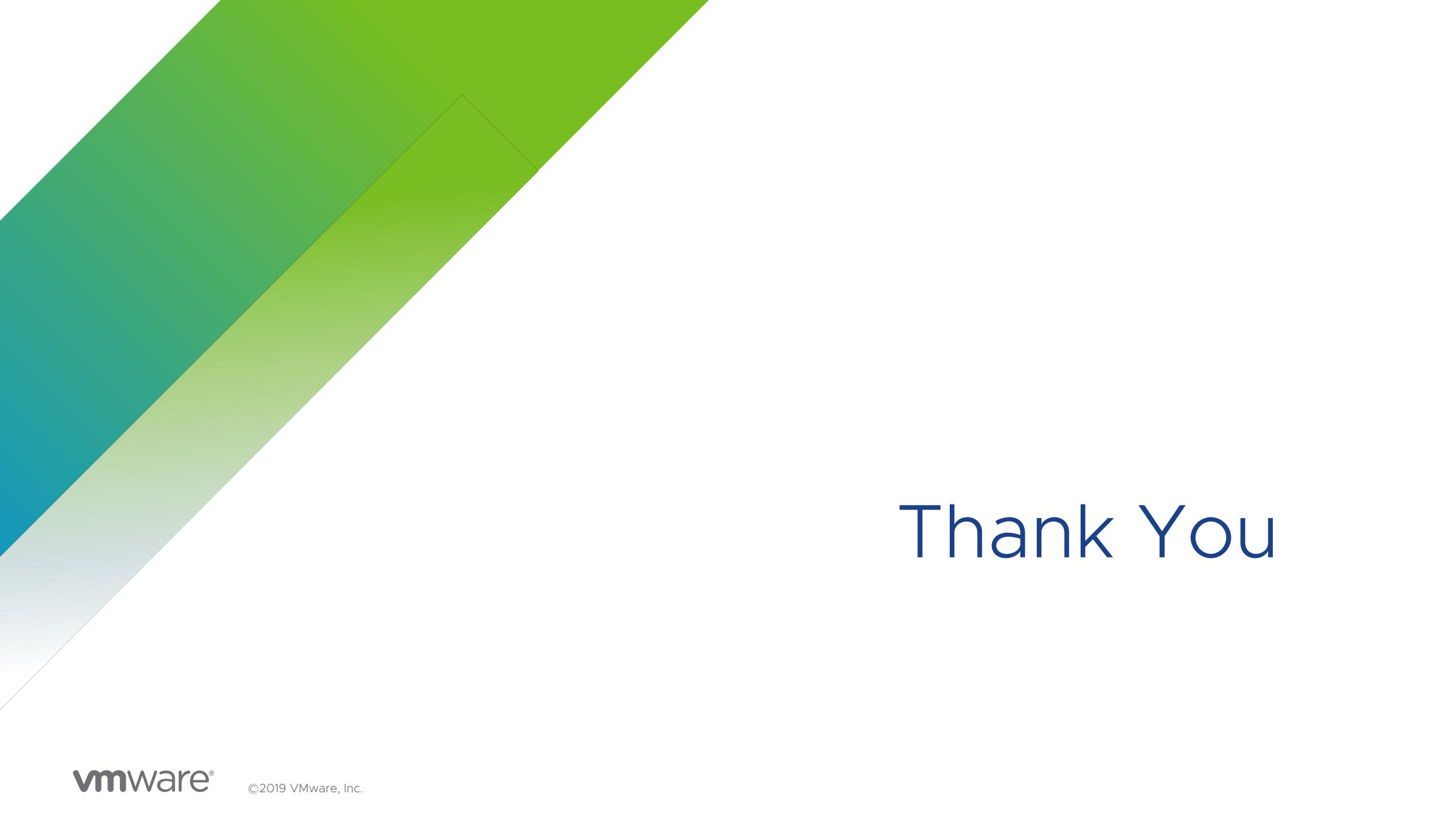
Network Service Mesh highlights

- Applying for a CNCF sandbox project - <https://github.com/cncf/toc/pull/212>
- Release planned for KubeCon EU in May, 2019
 - Stable basic functionality
 - VPP based dataplane
 - Verified scenarios

Want to know more?

Network Services Mesh Community

- Website - <https://networkservicemesh.io>
- Github - <https://github.com/networkservicemesh/networkservicemesh/>
- Weekly community calls - WG, Documentation, Use-cases
- IRC: #networkservicemesh on Freenode
- Upcoming Slack channel



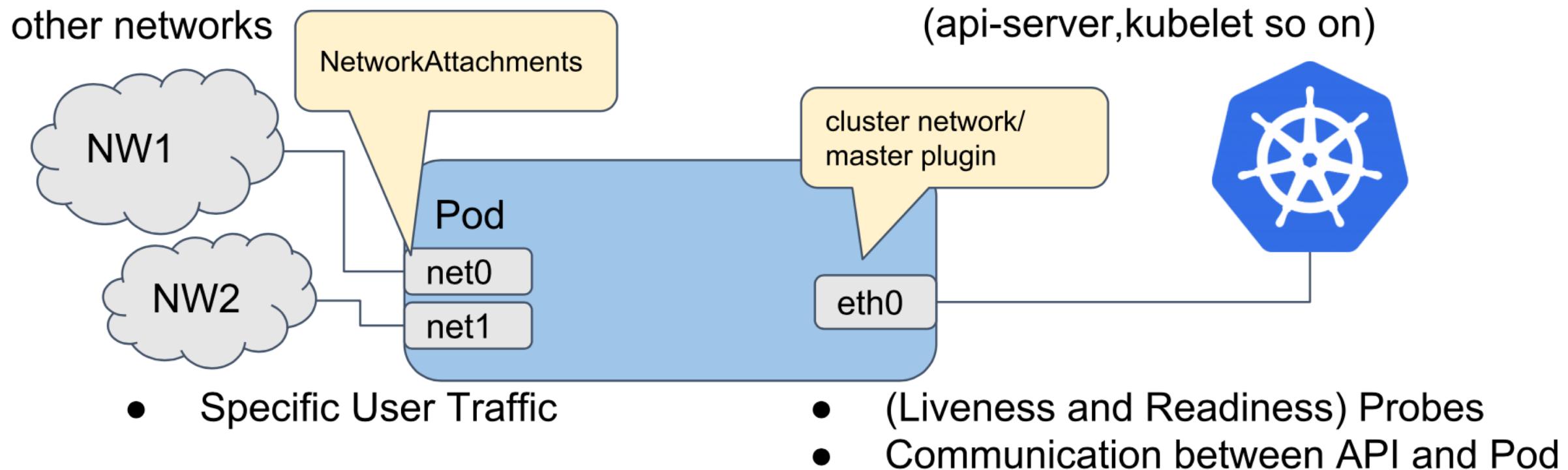
A decorative graphic in the top-left corner features a large, thin triangle pointing towards the top-right. The triangle is composed of several overlapping colored bands: a dark teal band at the bottom, followed by light green, medium green, and bright lime green bands at the top. The background behind the triangle is white.

Thank You

Networking in Kubernetes

Multus CNI

- Multiple CNI interfaces
- Services defined only on eth0



Networking in a Service Mesh

How it works



CNI

- Single interface `eth0`
- Iptables
- Sidecar Application Proxy (*L4-L7*)
- Ref: <https://medium.com/devopslinks/understanding-how-envoy-sidecar-intercept-and-route-traffic-in-istio-service-mesh-20fea2a78833>

