

Beyond Connectivity

Network services for cloud operators

Travis Newhouse (@travis_newhouse)

Chief Architect

AppFormix



AppFormix provides analysis, management, and optimization tools that Enterprise Cloud Operators need to control their environment and deliver a self-service IT experience to their users.

Cloudy with a chance of DevOps

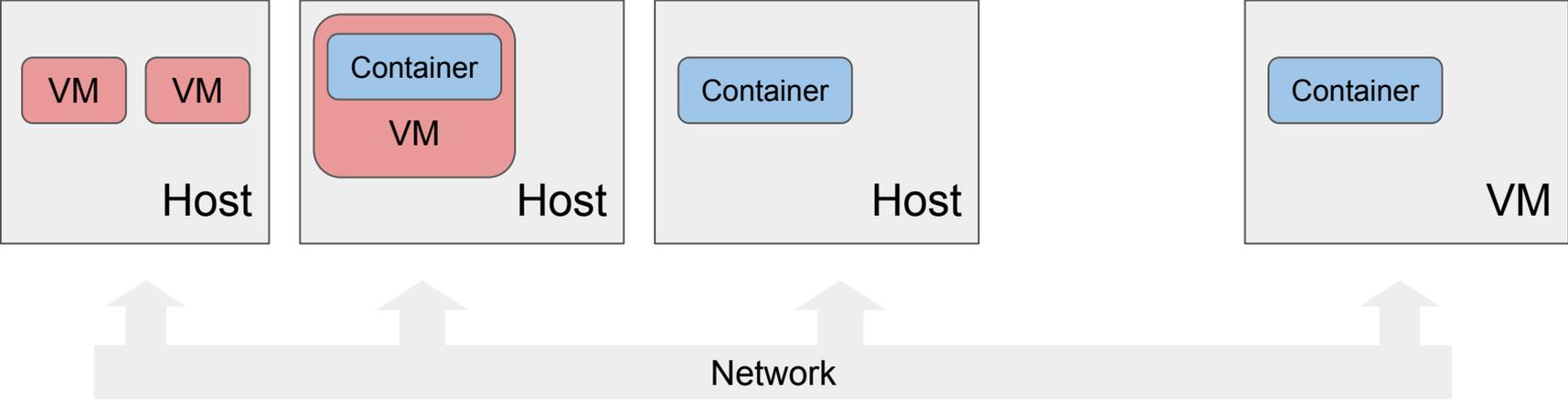
Amidst a technological and cultural shift

Dynamic infrastructure and micro-service architectures enabled by technologies like OpenStack and Kubernetes

Enterprise IT still wants complete control

Developers want choices for frictionless delivery

Enterprise Software-defined Data Center



Private cloud

Public cloud

Developers want...

- Applications to communicate
- SLA for minimum acceptable performance
- Choice of tools and platform

Don't want to worry about the network details.

Operators want...

- Resource management and capacity planning
- Ability to troubleshoot platform and infrastructure
- Fine-grained policies for access and resource utilization
- Self-service is ideal

Visibility into network

- What percent of connections are within same host?
- Which connections are being refused?
- Where is latency occurring?
- What applications are talking?
- What storage volumes using most bandwidth?
- What applications are under attack?

Microsegmentation

- Risk prevention inside the data center
 - security
 - regulatory compliance
- QoS, Resource allocation (go beyond simple access)
- Policy is expressed for an application
 - **not expressed as an IP address**
 - policy implemented where the application runs

What about SDN?

Decouple L4-L7 policy and services from L2/L3 connectivity

Network layer

- routing, switching, overlays
- L2/L3 network isolation

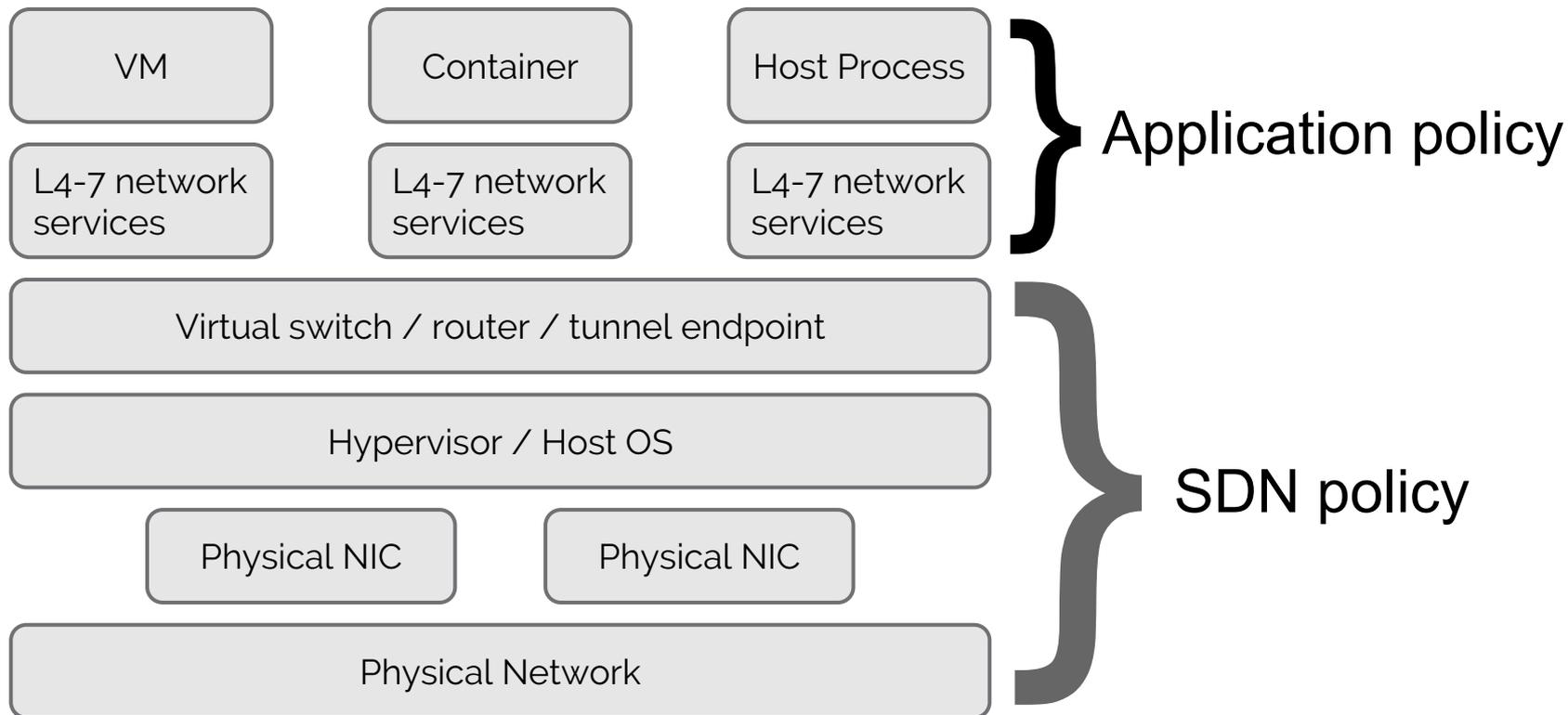
Application layer

- L4-L7 policy and services above virtual switch/router
- Services instantiated with the applications

Services at the edge

- At the edge, but part of the platform that Operators provide
 - below the VM or container
 - non-invasive to application and guest OS
- Services run on hosts and scale with the infrastructure
- Layer 4 and up services implemented after decapsulation or decryption
- Teams may not control the hardware or SDN (e.g., public cloud)
- Inline. Avoid hairpin mode to services outside of host.

Services at the edge



User-space, composable services

- Faster to innovate at user-space
- Easier to develop in user-space
- Long cycle from Upstream kernel acceptance to Distro to Enterprise
- Don't bloat the kernel
- Easier maintenance. Linux user ABI is stable.

Time to think about Network Services

Success of cloud native will depend on network services for operators

Empower quicker innovation and implementation of network services

Separate services and application policy from network layer

User-space, composable services at the edge