Policy Architecture and Framework for NFV Infrastructures

IETF 92

draft-norival-nfvrg-nfv-policy-arch-02

Co-authors
Norival Figueira – Brocade
Ram (Ramki) Krishnan – Dell
Diego Lopez – Telefonica I+D

Scope

- Discusses the policy architecture and framework to support NFV infrastructures
  - Where Policies are used to enforce business rules and specify resource constraints, e.g., energy constraints, in a number of subsystems, e.g., compute, storage, network, and etc., and across subsystems.
  - Where subsystems include the different “infrastructure domains” identified by the NFV ISG Infrastructure WG
- The focus is a policy architecture that uses known policy concepts and theories to address the unique requirements of NFV services including multiple NFV PoPs and networks
  - Focus is not general policy theory, which has already been intensively studied and documented on numerous publications over the past 10 to 15 years

Main Topics Covered by Current Draft

- Policy Intent Statement versus Subsystem Actions and Configurations
- Global vs Local Policies
- Hierarchical Policy Framework
- Policy Conflicts and Resolution
- Policy Pub/Sub Bus

Policy Intent Statement versus Subsystem Actions and Configurations

- The compliance statement in a policy may define actions
- Actions defined in a policy may be translated to subsystem *configurations*
- Example: “platinum treatment” may be translated to a specific QoS level treatment in a networking subsystem

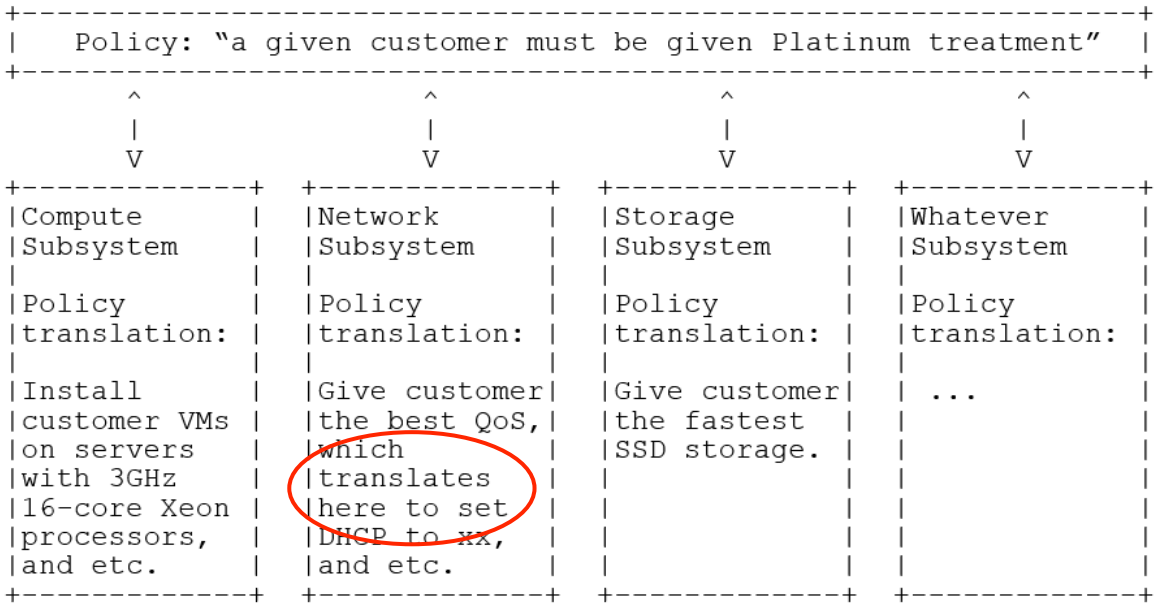

Figure 1: Example of Subsystem Translations of Policy Actions

Global vs Local Policies

- Policies may be subsystem specific in scope, while others may have broader scope and interact with multiple subsystems
- Example of compute-specific policy (local policy)
  - A specific customer is only allowed use certain server types for VNF/VM
- Example of broader scope policy (global policy)
  - A specific customer must be given “platinum treatment”

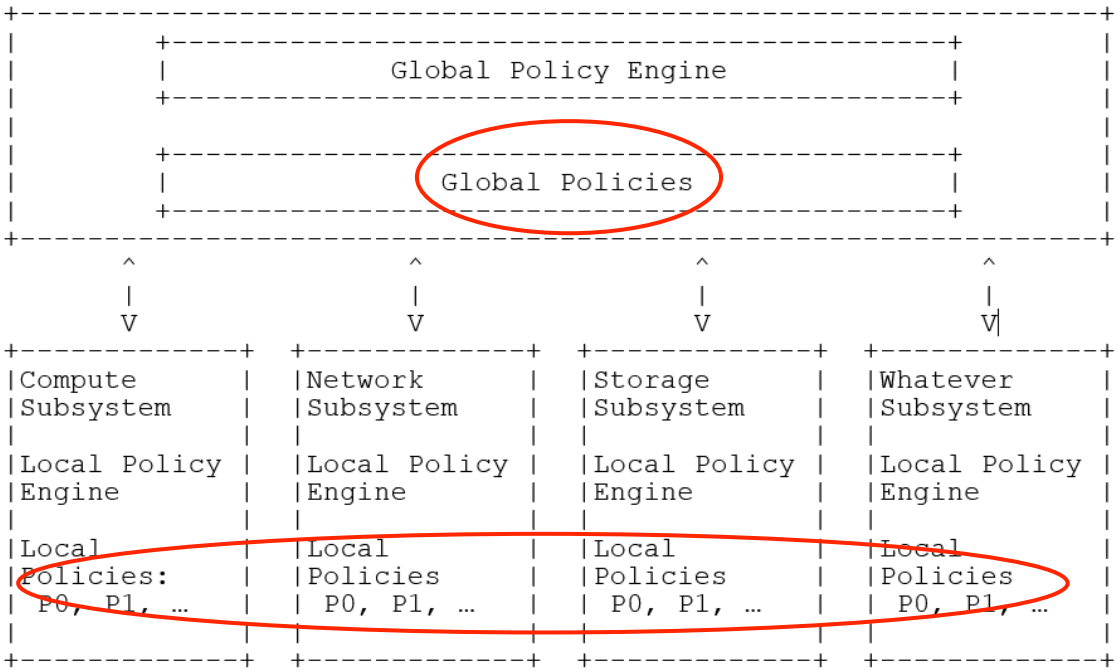

Figure 2: Global versus Local Policy Engines

Hierarchical Policy Framework

- The policy framework is hierarchical in nature, where the policy engine of a subsystem may be viewed as a higher level policy engine by lower level subsystems
  - e.g., Neutron would be a lower level subsystem in the OpenStack subsystem
- Multiple Data Center subsystems could be grouped in a region containing a region global policy engine
- One could define regions inside regions, hierarchically

We use the term “subsystem” here to loosely refer to any node in the hierarchy regardless of their functionality

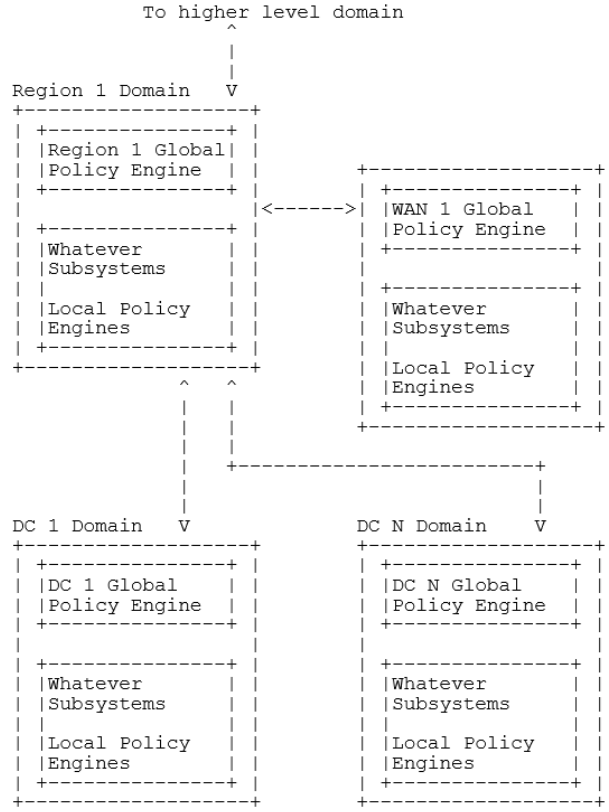

Figure 3: A Hierarchical Policy Framework

Policy Conflicts and Resolution

- As a new policy is added to a subsystem, its policy engine should perform conflict checks
- Example: A simple conflict would be created if new policy P1 is added after existing policy P2
  - P1: “customer *A* must not be allowed to use VNF *X*”
  - P2: “customer *A* is allowed to use VNF *X*”
  - The conflict should be detected and an appropriate policy conflict resolution mechanism should be initiated
- More complex conflicts may arise depending on how new policies are entered, e.g., manually vs. batched)
- Thus, there is a need for a reactive and preemptive policy conflict resolution mechanisms

Policy Pub/Sub Bus

- More subtle policy conflicts are possible between global and local policies
  - Compute local policy:
    “Platinum treatment must be provided using server of type *A*.”
  - Global policy
    “Platinum treatment must be provided using server subtype *A-1*”
- The above example demonstrate the need for subsystems to subscribe to policy updates at the Global policy level
- A *policy publication/subscription (pub/sub) bus* would be required
- A policy conflict may force policies to change scope (see draft for example)

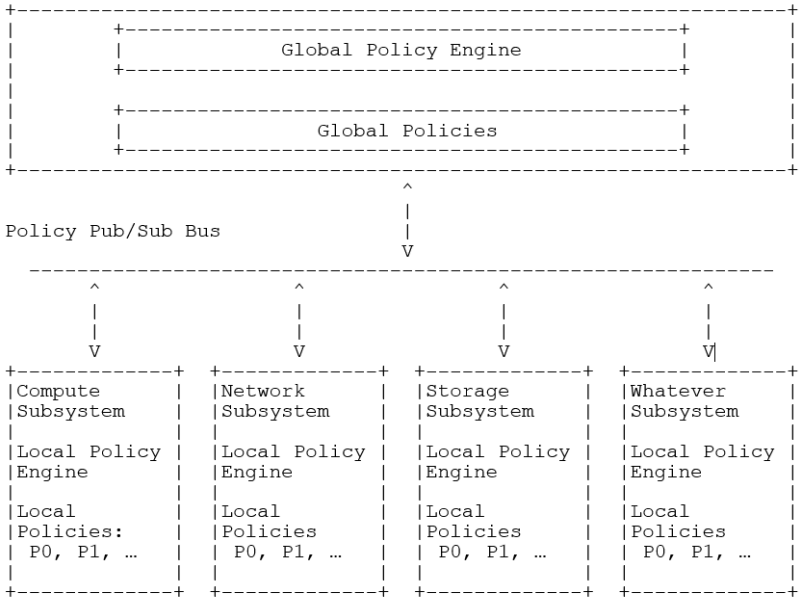

Figure 4: A Policy Pub/Sub Bus

Summary and Next Steps

- Draft analyzed policy scope, global versus local policies, policy actions and translations, policy conflict detection and resolution, interactions among policies engines, and a hierarchical policy architecture/framework to address the demanding and growing requirements of NFV environments, applicable as well to general cloud infrastructures
- The proposed policy architecture is also applicable to enterprises
  - e.g., a branch office could have capacity and energy constraints similar to that of many service provider NFV PoPs in constrained environments
  - This is an aspect that would be worth examining in detail in future work
- Related NFVRG draft – NFVIaaS architecture for policy based resource placement and scheduling
- An analysis of different conflict resolution strategies and their relationship with the policy pub/sub mechanisms
- RG adoption