May 2014

Network Policy

Abstractions in Neutron

Mohammad Banikazemi
Sumit Naiksatam
Stephen Wong

Outline

- Introduction
- Neutron Abstractions
- Group Policy Extension
- PoC Implementation and Demo
- Future Directions
- Q&A

Networking in the Cloud

- Current API: network centric
- Need a more application centric set of abstractions as well
  - More easily understood / utilized by higher layers
  - Declarative model
  - Separation of concerns

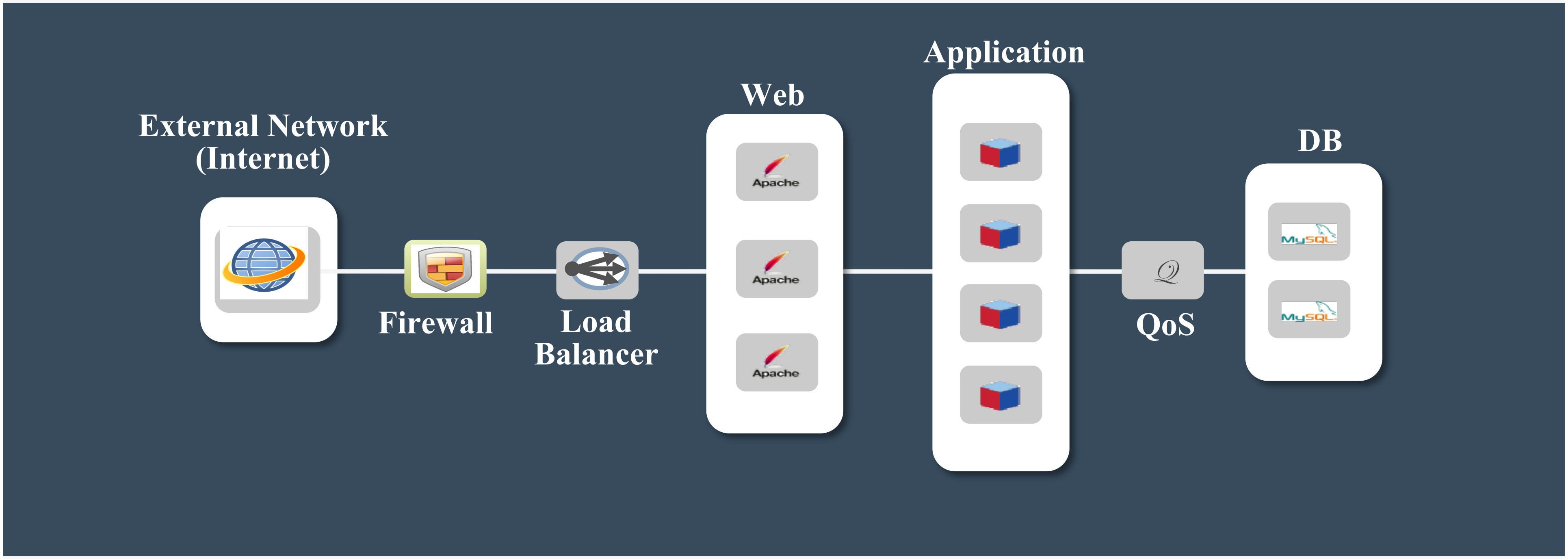
Desired Features

- Provide policy-based connectivity between application tiers
- Support dynamic application of policies
- Redirection to Network services and chains
- Policies defined by administrators and users

Current Neutron API

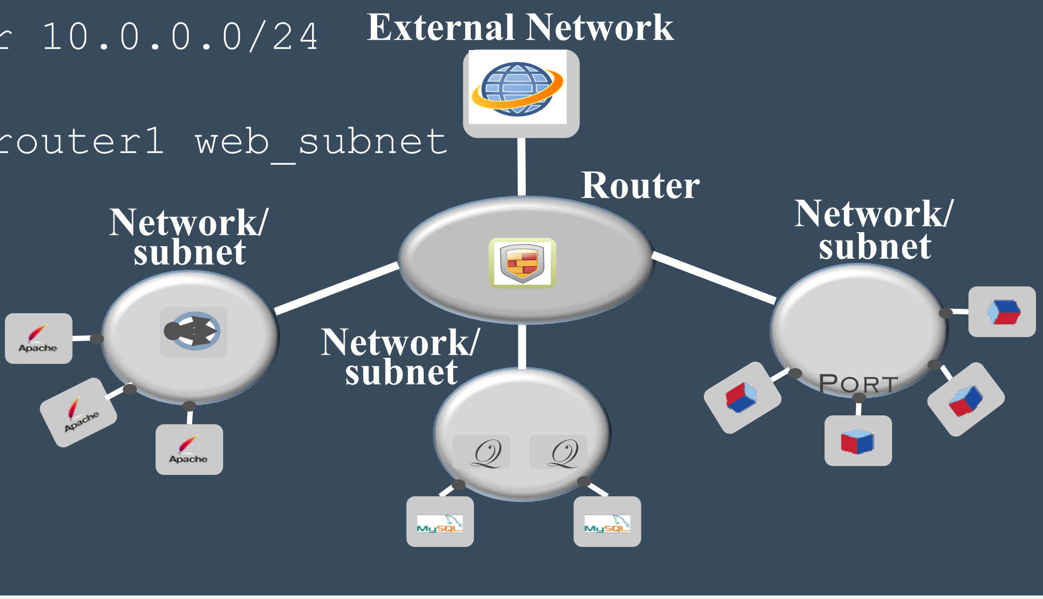
- Network centric, close to physical devices
  - Network: isolated layer-2 broadcast domain; private/shared
  - Subnet: CIDR IP address block associated with a network; optionally associated with gateway, DNS/DHCP servers
  - Port: virtual switch port on a network; has MAC and IP address properties
  - Router: connects networks, supports SNAT

Example: Multi Tier Apps



Neutron Representation

```
neutron net-create web_tier
neutron subnet-create web_tier 10.0.0.0/24
neutron router-create router1
neutron router-add-interface router1 web_subnet
. . .
```

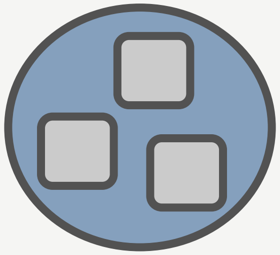


Group Policy

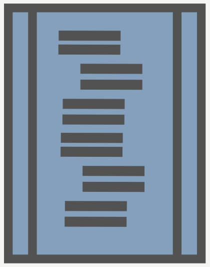
extension

The Basic Idea

- Endpoint (EP): Lowest unit of abstraction where policy is applied
- Endpoint Group (EPG): Logical grouping of endpoints



- Policy Rule: Network policies to access EPGs
- Contract: Collection of policy rules



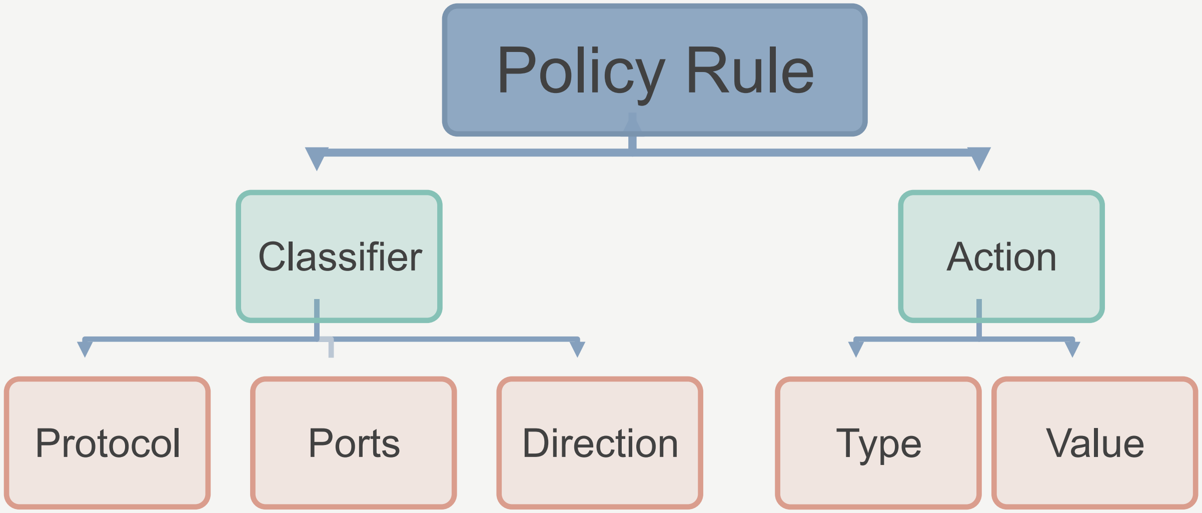
EPG-Contract Relationship

- Application deployer focused
- An EPG may provide one or more contracts
- An EPG may consume one or more contracts

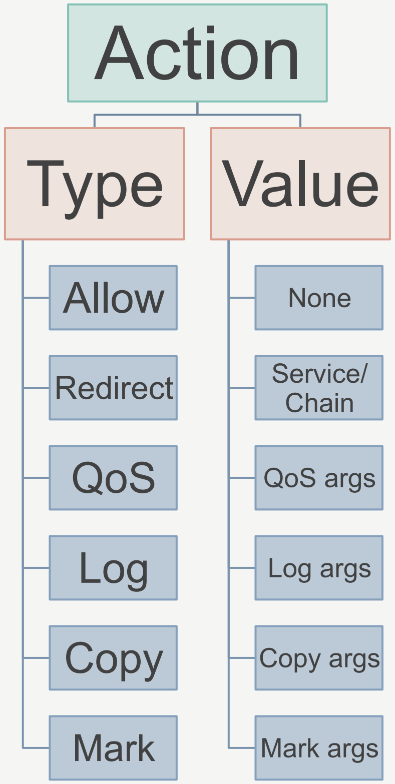
Endpoint Group

Contract

Policy Rules



- Policy Rule
  - Classifier
    - Protocol
    - Ports
    - Direction
  - Action
    - Type
    - Value



Action

Type	Value
Allow	None
Redirect	Service/ Chain
QoS	QoS args
Log	Log args
Copy	Copy args
Mark	Mark args

- Action is applied to traffic specified by Classifier

Group Policy - Workflow

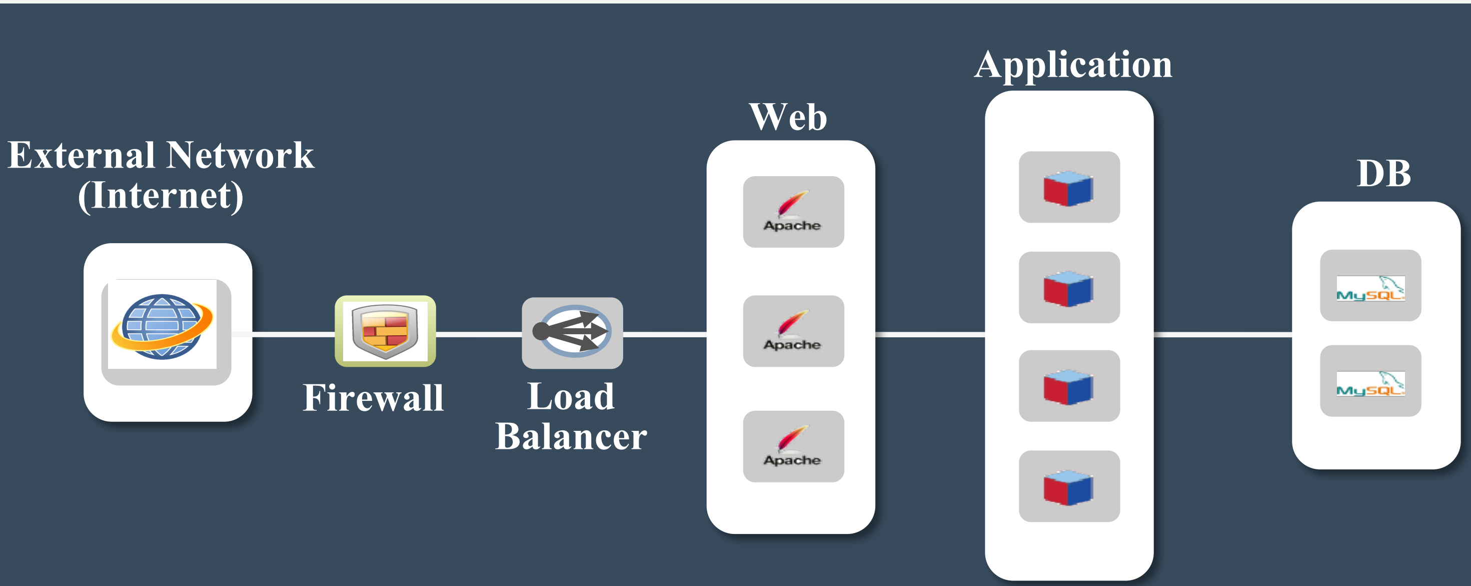
- Create contract

```
neutron classifier-create Insecure-Web-Access --port 80 --protocol TCP --direction IN

neutron policy-rule insecure-web --policy-classifier Insecure-Web-Access --actions ALLOW

neutron contract-create Web-Server-Contract --policy-rule  insecure-web
```

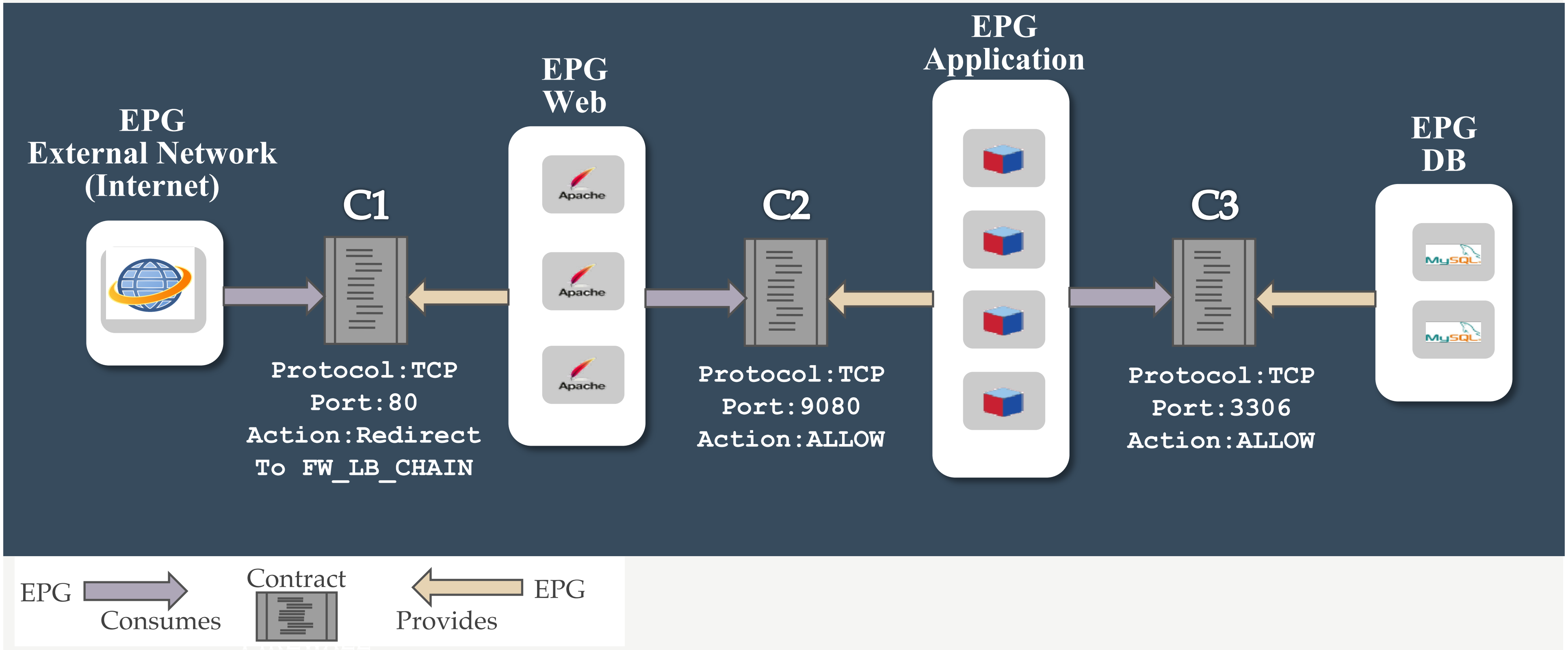
- Create EPGs and provide/consume contracts

```
neutron epg-create Web-Server-EPG --provides-contract Web-Server-Contract

neutron ep-create --endpoint-group Web-Server-EPG

neutron epg-create Outside-EPG --consumes-contract Web-Server-Contract
```

Putting It All Together – 3 Tier App



Group Policy Realization



EPG
External Network
(Internet)

C1

Protocol:TCP
Port:80
Action:Redirect
To FW_LB_CHAIN

EPG
Web

C2

Protocol:TCP
Port:9080
Action:ALLOW

EPG
Application

C3

Protocol:TCP
Port:3306
Action:ALLOW

EPG
DB

EPG Consumes

Contract

Provides EPG

Optional Constructs in Model

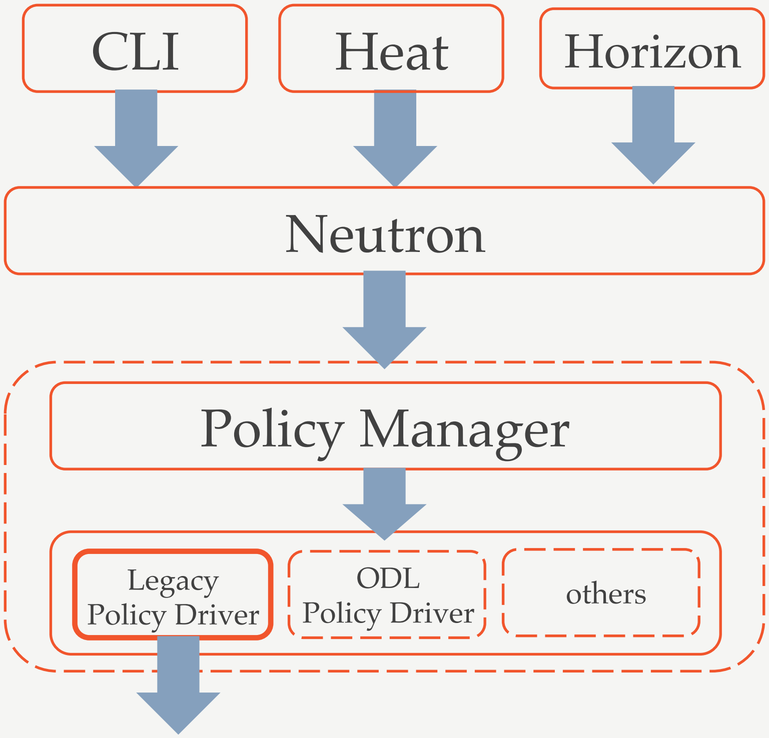
- **Scopes:** put constraints around how provider and consumer EPGs are matched
- **Policy Rule Filters:** allow for tagging Policy Rules with Labels such that subsets can be created in a Contract
- **Contract hierarchy:** infra admin constraints can be achieved by Contract hierarchical composition
- **Endpoint labels:** policies get triggered automatically when labels are added or removed

Proof of Concept

implementation

PoC Implementation

- Team has worked on a PoC implementation
- Considering various model and implementation alternatives
- Using legacy driver
- CLI, Horizon, and Heat



The Group Policy PoC Team

- Sumit Naiksatam, Robert Kukura, Mandeep Dhami (Cisco)
- Mohammad Banikazemi (IBM)
- Stephen Wong (Midokura)
- Ronak Shah (Nuage Networks)
- Hemanth Ravi, Susaant Kondapaneni, Prasad Vellanki (One Convergence)
- Rudra Rugge (Juniper)

State of Implementation

- The blueprint for Group Policy has been reviewed/approved
- Working PoC available (install from: https://github.com/noironetworks/devstack/tree/group-policy-poc)
- Neutron reference implementation for Group Policy is in progress
- Complementary work on network services framework is in progress

More Information

- Neutron Group-based Policy design session
  May 16 • 10:50am - 11:30am • B304

- Wiki page:
  https://wiki.openstack.org/wiki/Neutron/GroupPolicy

- Neutron Group Policy Sub-Team Meeting IRC weekly meetings:
  https://wiki.openstack.org/wiki/Meetings/Neutron_Group_Policy