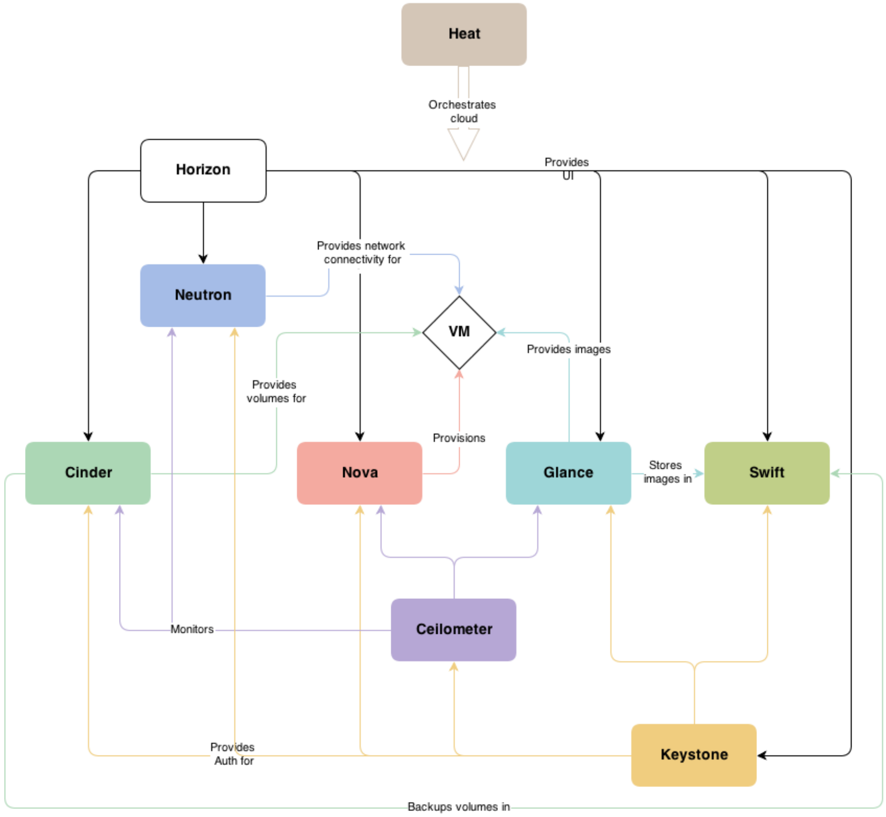
OpenStack Network Service

Codename: Neutron

rackspace®

the open cloud company

Neutron Overview



OpenStack Network Service

Neutron

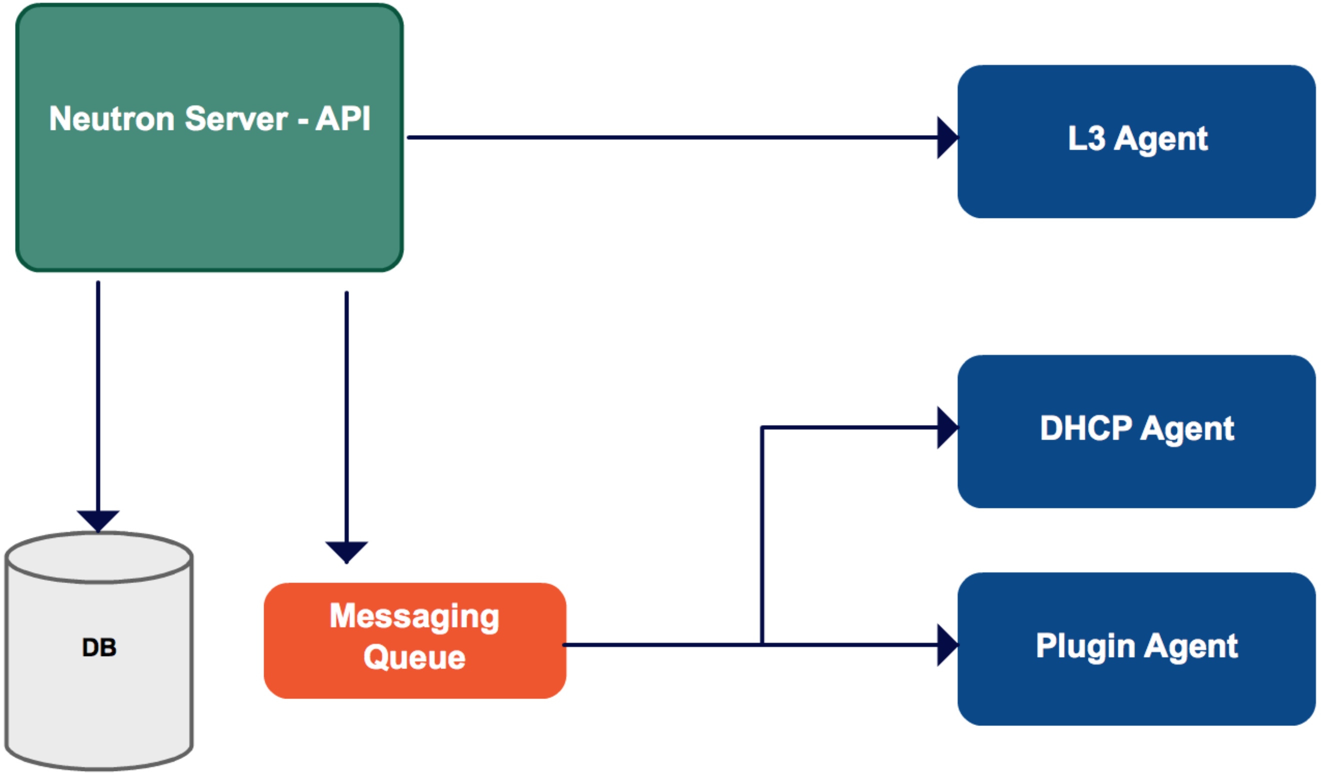
Pluggable, scalable, API-driven network and IP management

Provides a rich and tenant-facing API for defining network connectivity and addressing in the cloud.

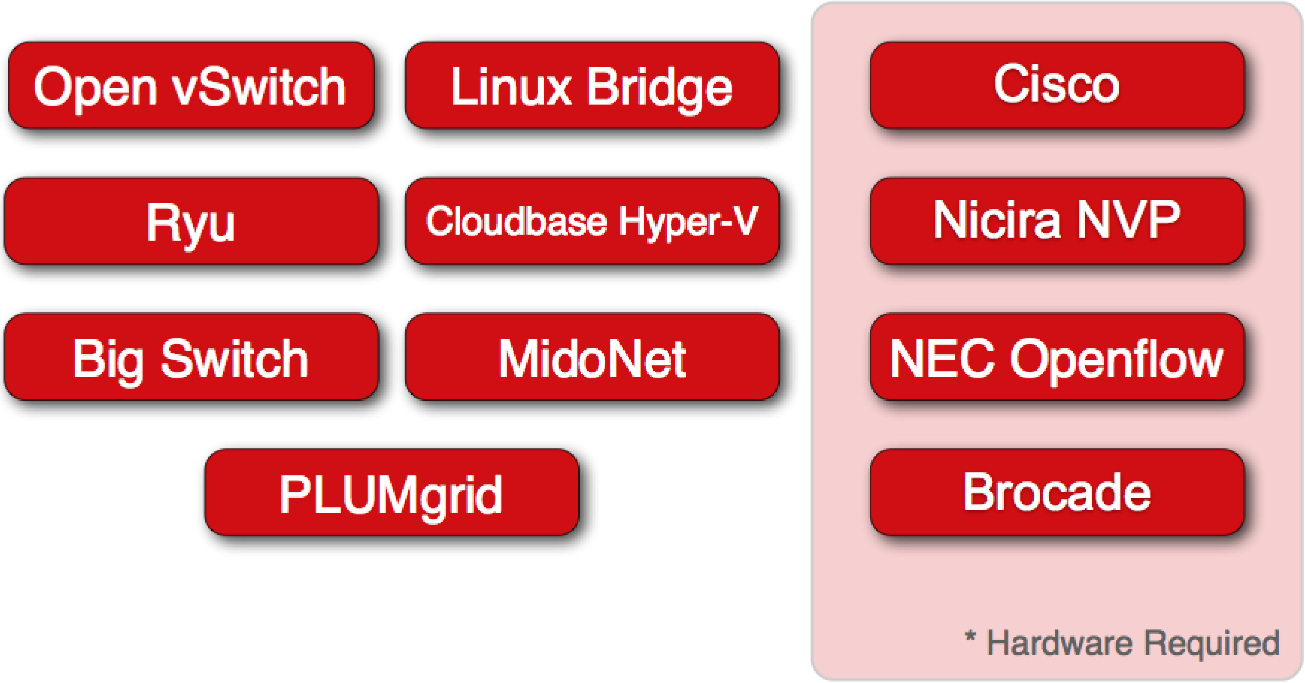
Neutron Resources

- **Network**
  An isolated L2 segment, analogous to a VLAN in physical networking
- **Subnet**
  A block of v4 or v6 IP addresses and associated configuration state
- **Port**
  A connection point for attaching a single device (NIC) to a Neutron network

Neutron Components



Neutron Plugins



Open vSwitch

Linux Bridge

Ryu

Cloudbase Hyper-V

Big Switch

MidoNet

PLUMgrid

Cisco

Nicira NVP

NEC Openflow

Brocade

* Hardware Required

Open vSwitch Plugin

- **Multilayer virtual switch**
  - Released under the Apache 2.0 license
- **Enables massive network automation through programmatic extensions**
- **Supports standard management interfaces**
  - NetFlow
  - sFlow
  - SPAN
  - RSPAN
  - CLI
  - LACP
  - 802.1ag
- **Supports standard protocols**
  - VLAN and GRE
  - OpenFlow
- **Supports distribution across multiple physical servers**
- **Supports software only and mixed network solutions**

Linux Bridge Plugin

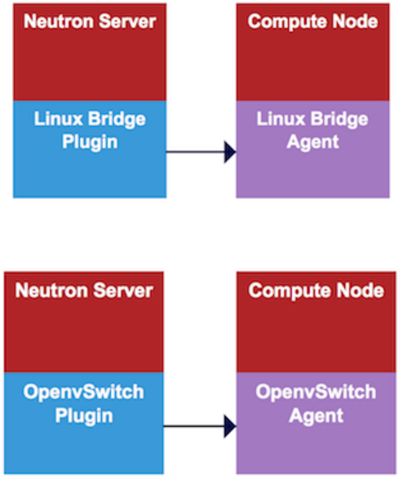
- Uses Linux L2 bridging and VLANS
- Compatible with Nova Networks
- Does not scale well across multiple compute nodes

ML2 Plugin Framework

One of the most significant features of the Havana release was the introduction of the ML2 (Modular Layer 2) plugin framework.

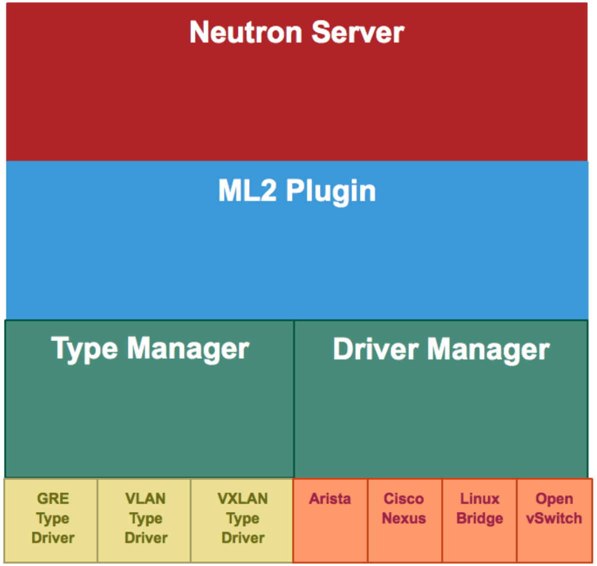
This allows OpenStack Networking to utilize a variety of existing layer 2 agents instead of locking into one specific vendor plugin.

Pre-ML2 Monolithic Plugin

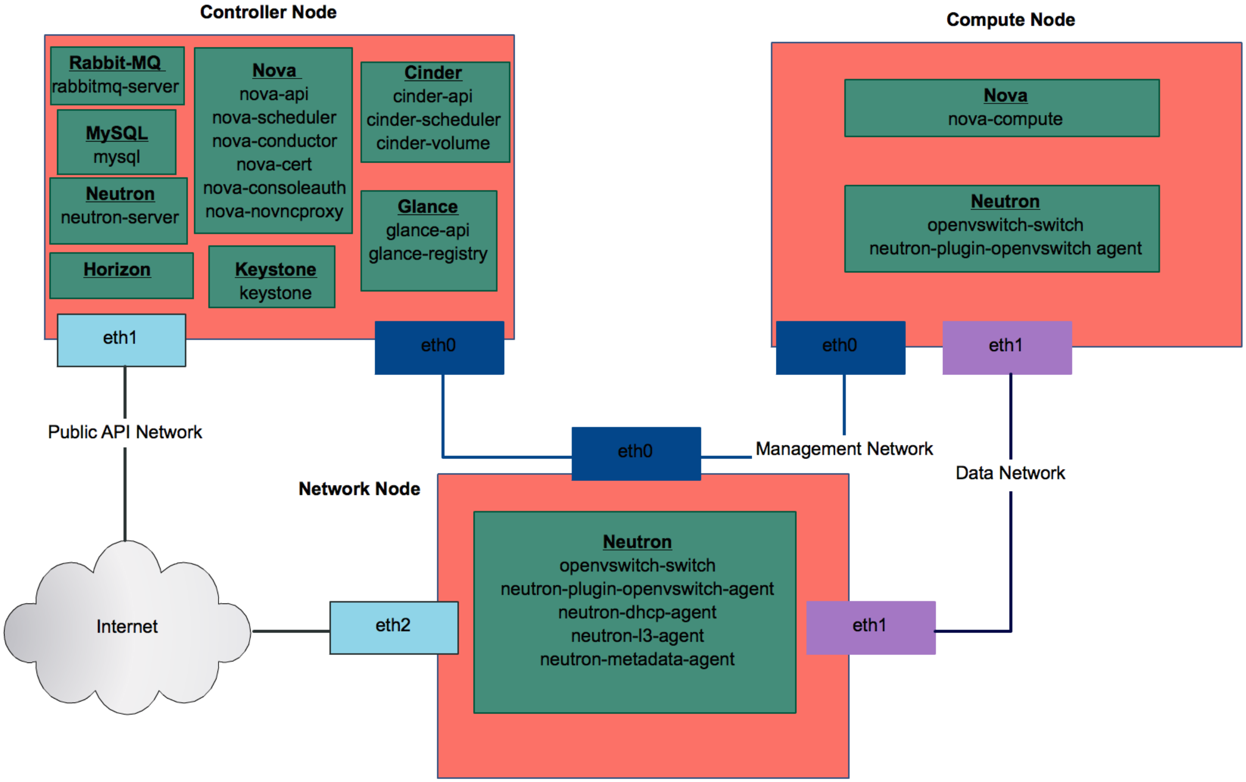


ML2 Architecture

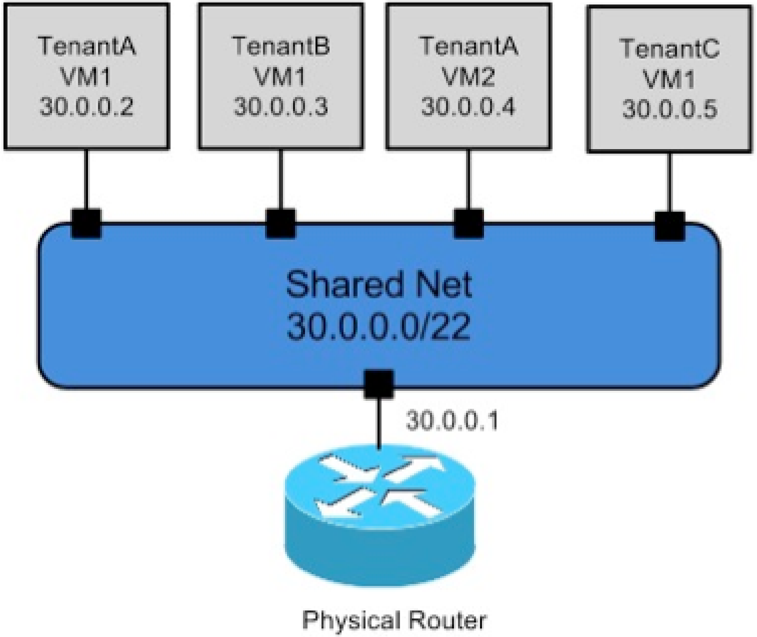
The ML2 introduces the use of Type and Driver Managers to allow for the use of variety of vendors and networking technologies:



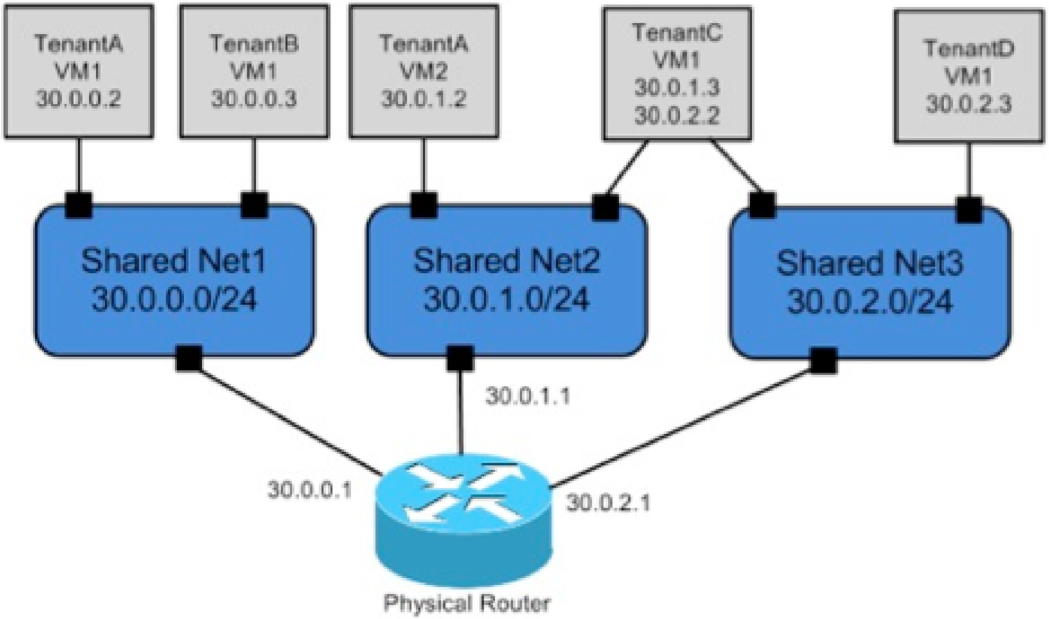
Neutron Network Connectivity



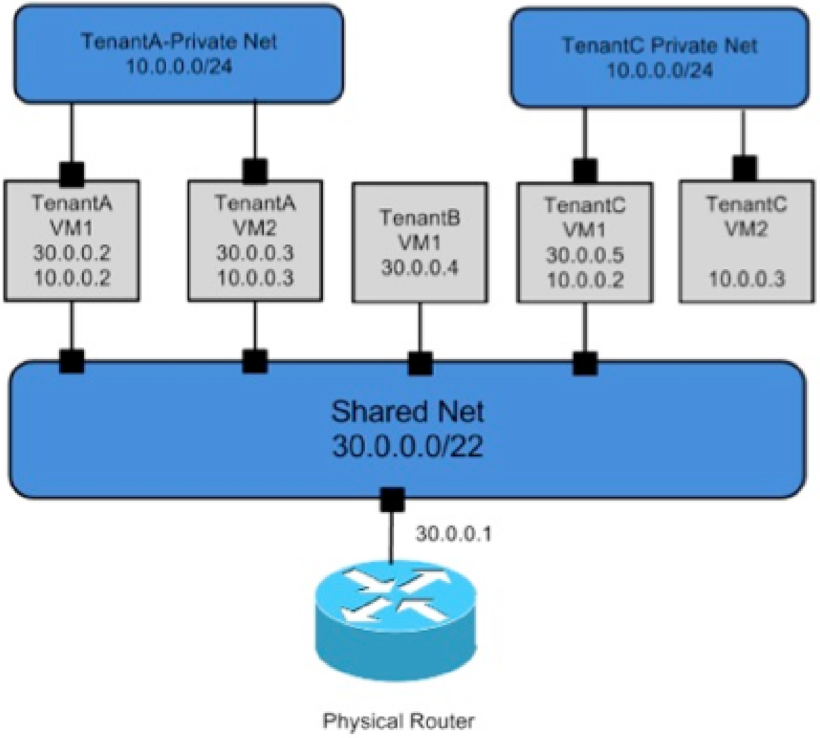
Use Cases: Single Flat Network



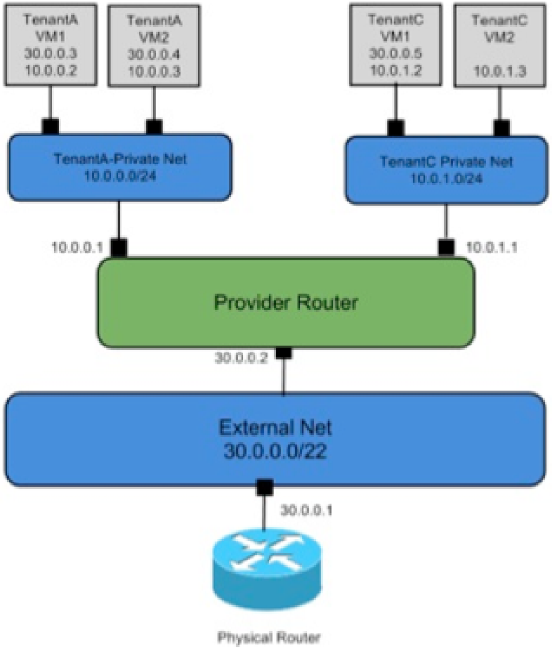
Use Case: Multiple Flat Networks



Use Case: Mixed Flat Private Network

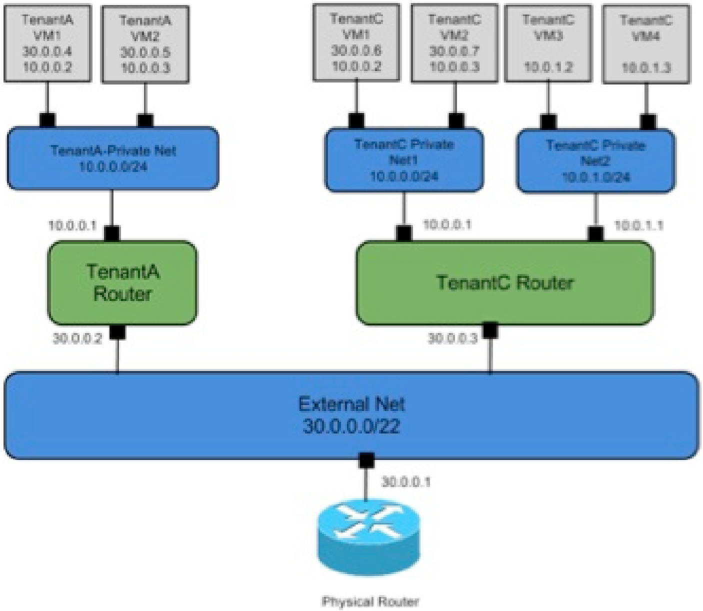


Use Case: Provider Router with Private Networks

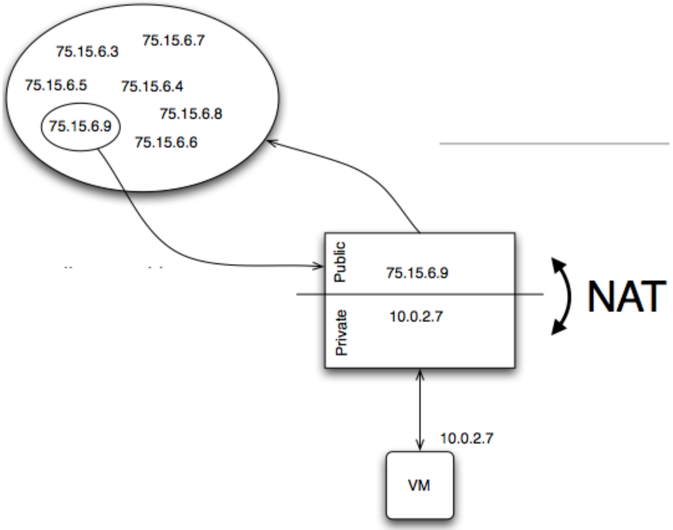


the open cloud company

Use Case: Per Tenant Router with Private Networks

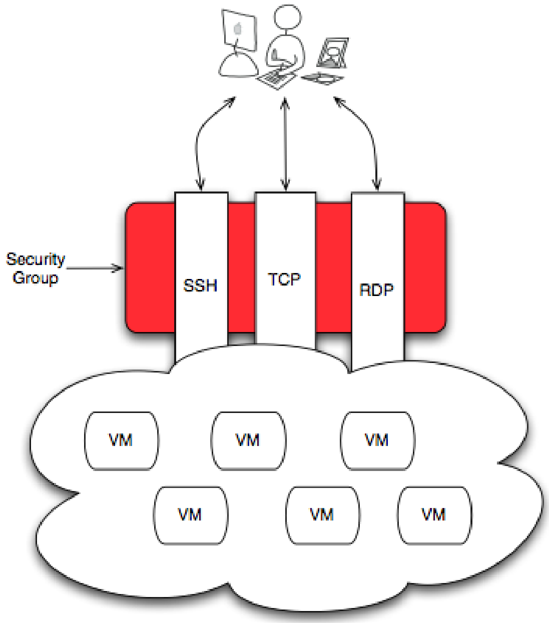

TenantA VM1 30.0.0.4 10.0.0.2
TenantA VM2 30.0.0.5 10.0.0.3
TenantC VM1 30.0.0.6 10.0.0.2
TenantC VM2 30.0.0.7 10.0.0.3
TenantC VM3 10.0.1.2
TenantC VM4 10.0.1.3
TenantA-Private Net 10.0.0.0/24
TenantC Private Net1 10.0.0.0/24
TenantC Private Net2 10.0.1.0/24
10.0.0.1
10.0.0.1
10.0.1.1
TenantA Router
TenantC Router
30.0.0.2
30.0.0.3
External Net 30.0.0.0/22
30.0.0.1
Physical Router

L3 Router & Floating IPs



- Basic L3 router construct to route between L2 networks
- Provides a gateway to external networks
- Support for SNAT and Floating IPs

Security Groups



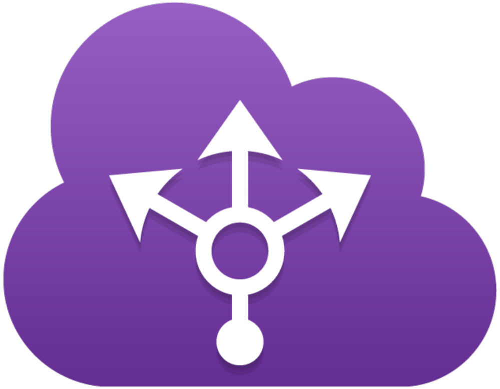
- Allows L3-L4 packet filtering to protect virtual machines.
- Network access rules that specify traffic allowed to and from a VM
- Associated with a VM at startup
    - If not specified, a VM is assigned to the default Security Group,which allows traffic from all other members of the group
- VMs can be associated with many Security Groups
- Security Group rule specifies:
    - Source of traffic (IP/CIDR or another Security Group)
    - Protocol (TCP, UDP, ICMP)
    - Destination port on VM

Security Groups

- **Moved to Neutron project in Grizzly**
- **Backward compatible with Nova-API**
- **Additional features not found in Nova:**
    - IPv6 and IPv4 support
    - Inbound + outbound filtering
    - Overlapping IP address range support
    - Can be offloaded by plugins to enhanced filtering engines rather than iptables

Load-balancing-as-a-Service (LBaaS)

- Full load balancing API model + pluggable framework
- Basic implementation based on HAproxy
- Working with leading vendors on additional plugins
- Work in progress



rackspace® the open cloud company

Firewall-as-a-Service (FWaaS)

Havana introduced Firewall-as-a-Service and VPN-as-a-Service.

FWaaS implements firewall rules with the use of Iptables. The Iptables configuration will be realized by an agent-driver combination that will program the Iptables rules on a gateway host. This agent is collocated with the L3 agent.

FWaas is a perimeter firewall distributed one per tenant. Creating a firewall stays in pending state until a router is created and the firewall is applied to that router.

- Here are some examples:

```
neutron firewall-rule-create --protocol TCP --destination-port 80 --action allow webrule
neutron firewall-rule-create --protocol TCP --destination-port 22 --action allow sshrule
neutron firewall-policy-create --firewall-rules webrule sshrule mypolicy
neutron firewall-rule-create --protocol TCP --destination-port 22 --action allow sshrule
```

VPN-as-a-Service (VPNaaS)

The VPNaaS extension provides OpenStack tenants with the ability to extend private networks across the public telecommunication infrastructure. The capabilities provided by this initial implementation of the VPNaaS extension are:

- Site-to-site Virtual Private Network connecting two private networks.
- Multiple VPN connections per tenant.