FWass

**Firewall-as-a-Service**

firewall-as-a-service(FWaaS)网络插件将防火墙应用于OpenStack对象，例如项目、路由器和路由器端口。

OpenStack防火墙的核心概念是防火墙策略和防火墙规则的概念。策略是规则的有序集合。规则指定组成匹配标准的属性集合(如端口范围、协议和IP地址)，并在匹配的流量上执行(允许或拒绝)。一个策略可以公开，因此可以跨项目共享。

防火墙以不同的方式实现，取决于所使用的驱动程序。例如，iptables驱动程序使用iptable规则实现防火墙。OpenVSwitch驱动程序在流表中使用流条目实现防火墙规则。一个Cisco防火墙驱动程序操纵NSX设备。

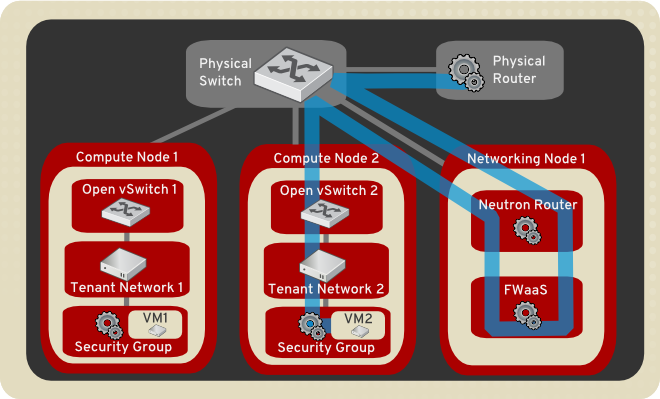
**IPtables作用于内外网，安全组作用于内网；相较于安全组IPtables配置更加细化，可以具体细化到某台实例。**

## **FWaaS有v1和v2两个版本，v2版某些功能不成熟，v1版有dashboard界面**

## **FWaaS v1**

最初的FWaaS实现v1，为路由器提供保护。当防火墙被应用到路由器时，所有内部端口都受到保护。

下图描述了FWaaS v1保护。它举例说明了VM2实例的入口流量和出口流量:



**FWaaS v2**

更新的FWaaS实现v2提供了更细粒度的服务。防火墙的概念已经被防火墙组取代，以表明防火墙由两个策略组成:一个ingress策略和一个出口策略。防火墙组不是在路由器级别(在路由器上的所有端口)上应用，而是在端口级别上应用。目前，可以指定路由器端口。对于Ocata，也可以指定VM端口。

**FWaaS v1 对比 v2**

下表比较了v1和v2特性：

|  |  |  |
| --- | --- | --- |
| **特性** | **v1** | **v2** |
| 支持路由器的L3防火墙 | YES | NO\* |
| 支持路由器端口的L3防火墙 | NO | YES |
| 支持L2防火墙(VM端口) | NO | NO\*\* |
| 命令行接口支持 | YES | YES |
| 图形界面支持 | YES | NO |

\*一个防火墙组可以应用于给定路由器上的所有端口，以达到这个目的。

\*\*此功能是为Ocata计划的。

启用v1版

1、安装fwaas插件包

#yum install openstack-neutron-fwaas -y

2、修改相关配置文件

①/etc/neutron/neutron.conf中启用fwaas插件

[DEFAULT]

service\_plugins = router,firewall

②/etc/neutron/fwaas\_driver.ini中添加配置项

[fwaas]

agent\_version = v1

driver = iptables

enabled = True

③为L3代理配置fwaas插件

[AGENT]

extensions = fwaas

1. 在数据库中创建所需要的表

#neutron-db-manage --subproject neutron-fwaas upgrade head

1. 在dashboard中显示fwaas插件，配置/etc/openstack-dashboard/local-settings文件

OPENSTACK\_NEUTRON\_NETWORK = {

enable\_firewall : True

(开启所有flase为true,因为后面实现负载集群也需要开启）

}

重启Apache

#systemctl restart httpd

1. 重新启动neutron-l3-agent和neutron-server服务来应用这些设置

#systemctl restart neutron-l3-agent.service neutron-server