

前面我们学习了安全组，今天学习另一个与安全相关的服务 -- FWaaS。  
  
**理解概念**

Firewall as a Service（FWaaS）是 Neutron 的一个高级服务。  
用户可以用它来创建和管理防火墙，在 subnet 的边界上对 layer 3 和 layer 4 的流量进行过滤。

传统网络中的防火墙一般放在网关上，用来控制子网之间的访问。

FWaaS 的原理也一样，是在 Neutron 虚拟 router 上应用防火墙规则，控制进出租户网络的数据。

FWaaS 有三个重要概念：

Firewall、Policy 和 Rule。

**Firewall**租户能够创建和管理的逻辑防火墙资源。

Firewall 必须关联某个 Policy，因此必须先创建 Policy。

**Firewall Policy**Policy 是 Rule 的集合，Firewall 会按顺序应用 Policy 中的每一条 Rule。

**Firewall Rule**Rule 是访问控制的规则，由源与目的子网 IP、源与目的端口、协议、allow 或 deny 动作组成。  
例如，我们可以创建一条 Rule，允许外部网络通过 ssh 访问租户网络中的 instance，端口为 22。

与 FWaaS 容易混淆的概念是安全组（Security Group）。

安全组的应用对象是虚拟网卡，由 L2 Agent 实现，比如 neutron\_openvswitch\_agent 和 neutron\_linuxbridge\_agent。  
安全组会在计算节点上通过 iptables 规则来控制进出 instance 虚拟网卡的流量。  
也就是说：**安全组保护的是 instance**。

FWaaS 的应用对象是 router，可以在安全组之前控制外部过来的流量，但是对于同一个 subnet 内的流量不作限制。  
也就是说：**FWaaS 保护的是 subnet**。

所以，可以同时部署 FWaaS 和安全组实现双重防护。

**启用 FWaaS**

因为 FWaaS 是在 router 中实现的，所以 FWaaS 没有单独的 agent。

已有的 L3 agent 负责提供所有 FWaaS 功能。

要启用 FWaaS，必须在 Neutron 的相关配置文件中做些设置。

**配置 firewall driver**

Neutron 在 /etc/neutron/fwaas\_driver.ini 文件中设置 FWaaS 使用的 driver。

如下图所示：  
http://7xo6kd.com1.z0.glb.clouddn.com/upload-ueditor-image-20161124-1479989223520015826.jpg

这里 driver 为 iptables。如果以后支持更多的 driver，可以在这里替换。

**配置 Neutron**

在 Neutron 配置文件 /etc/neutron/neutron.conf  中启用 FWaaS plugin。

http://7xo6kd.com1.z0.glb.clouddn.com/upload-ueditor-image-20161124-1479989223586010684.jpg

配置完毕！下节我们开始创建 Firewall。