

Neutron 为 instance 提供了两种管理网络安全的方法：

安全组（Security Group）和虚拟防火墙。

安全组的原理是通过 iptables 对 instance 所在计算节点的网络流量进行过滤。

虚拟防火墙则由 Neutron Firewall as a Service（FWaaS）高级服务提供。

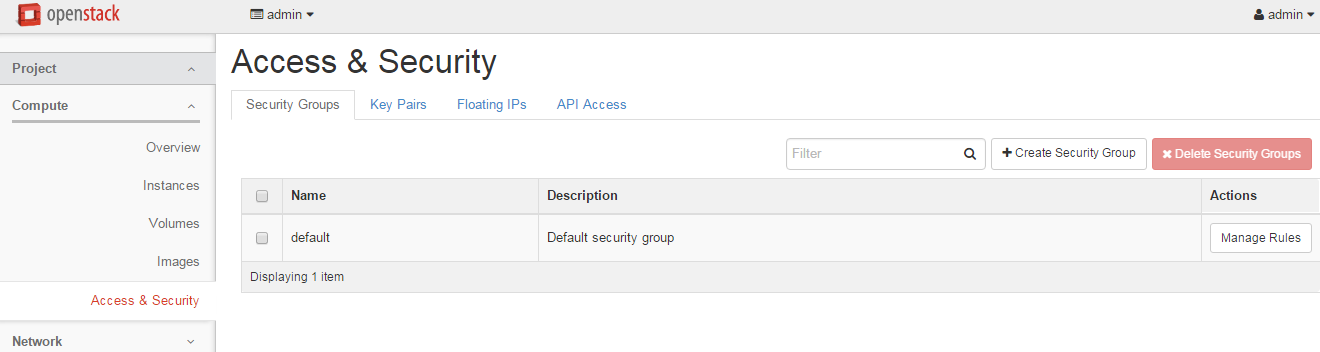
其底层也是使用 iptables，在 Neutron Router 上对网络包进行过滤。

这两种安全方案我们都会讨论，本章先重点学习安全组。

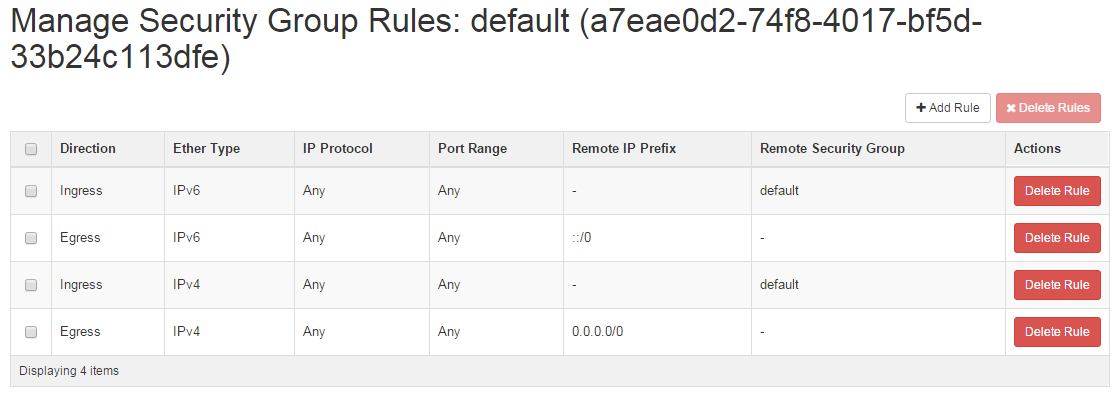
**默认安全组**

每个 Project（租户）都有一个命名为 “default” 的默认安全组。

点击菜单 Project -> Compute -> Access & Security，查看 Security Group 列表。



点击http://7xo6kd.com1.z0.glb.clouddn.com/upload-ueditor-image-20161119-1479556482194076108.jpg按钮，查看 “default” 安全组的规则。

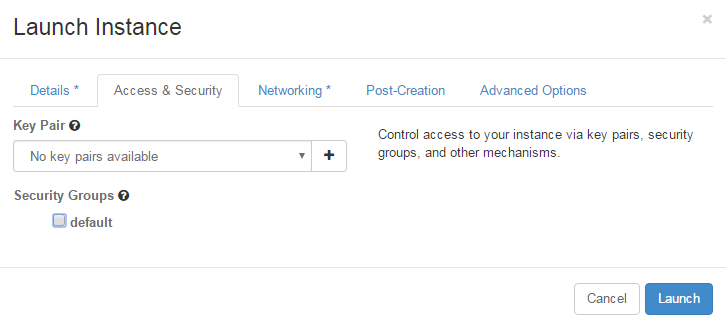


“default” 安全组有四条规则，其作用是：

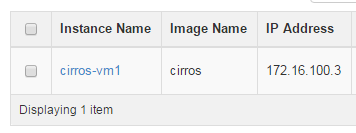
**允许所有外出（Egress）的流量，但禁止所有进入（Ingress）的流量。**

当我们创建 instance 时，可以在 “Access & Security” 标签页中选择安全组。

如果当前只有 “default” 这一个安全组，则会强制使用 “default” 。



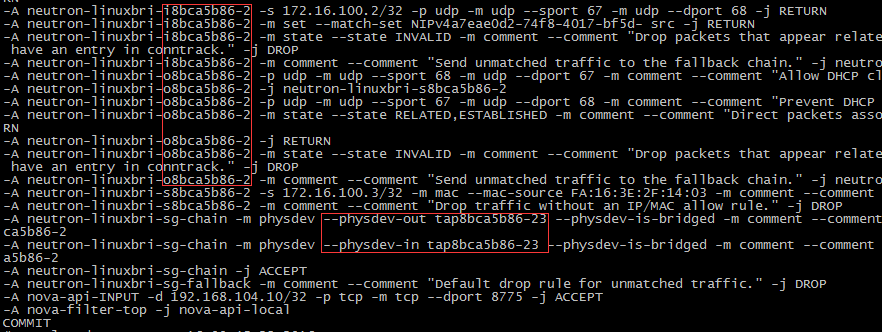
当前在 devstack-controller 上有 instance “cirros-vm1”。



在 devstack-controller 上执行 iptables-save 命令查看相关规则。

iptables 的规则较多，这里我们节选了 cirros-vm1 相关的规则。  
这些规则是 Neutron 根据安全组自动生成的。

如果大家想深入理解 iptables，可 google 相关文档。



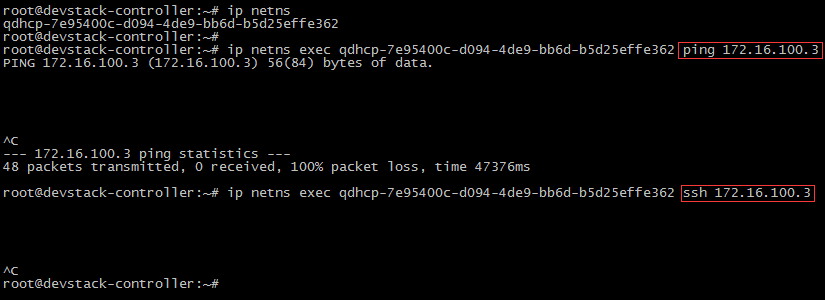
cirros-vm1 的 TAP interface 为 tap8bca5b86-23，可以看到：

1. iptables 的规则是应用在 Neutron port 上的，port 在这里是 cirros-vm1 的虚拟网卡 tap8bca5b86-23。

2. ingress 规则集中定义在命名为 “neutron-linuxbri-i8bca5b86-2” 的 chain 中。

3. egress  规则集中定义在命名为 “neutron-linuxbri-o8bca5b86-2” 的 chain 中。

下面我们通过 dhcp namespace 对 cirros-vm1 进行 ping 和 ssh 测试。



无法 ping 和 ssh cirros-vm1，可见当前的规则实现了 “default” 安全组，所有 ingress 流量都被禁止。

下节我们会创建新的安全组允许 ping 和 ssh。