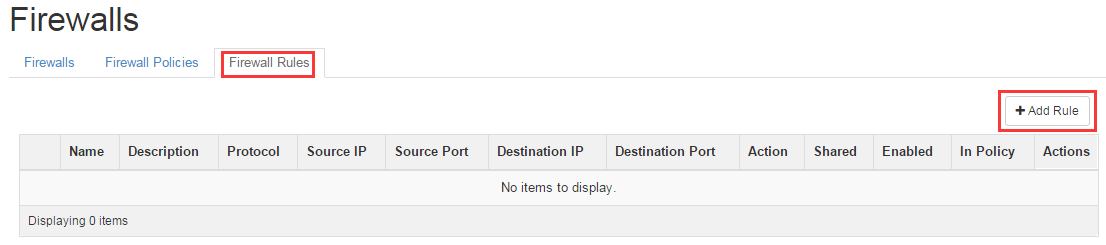


上一节应用了无规则的虚拟防火墙，不允许任何流量通过。

今天我们会在防火墙中添加一条规则，允许 ssh。  
最后我们会对安全组和 FWaaS 作个比较。

下面我们添加一条 firewall rule：允许 ssh。

在 Firewall Rules 标签页面点击 “Add Rule” 按钮。

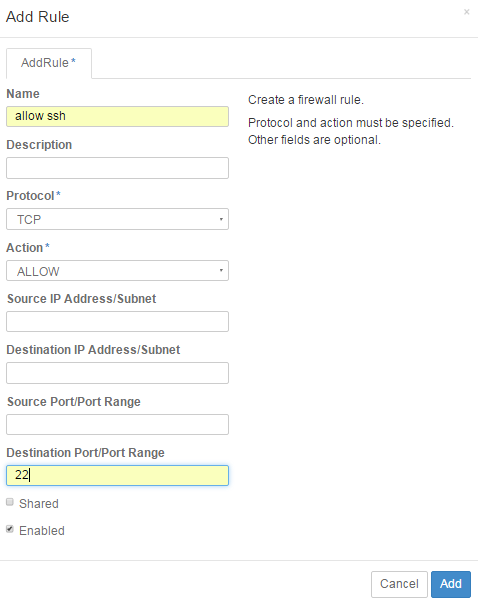


将新 rule 命名为 “allow ssh”，

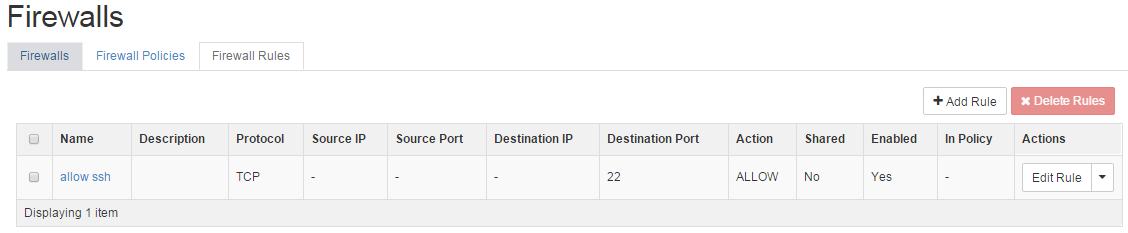
Protocal 选择 “TCP”，

Action 为 “ALLOW”，

Destination Port/Port Range 为 “22”，

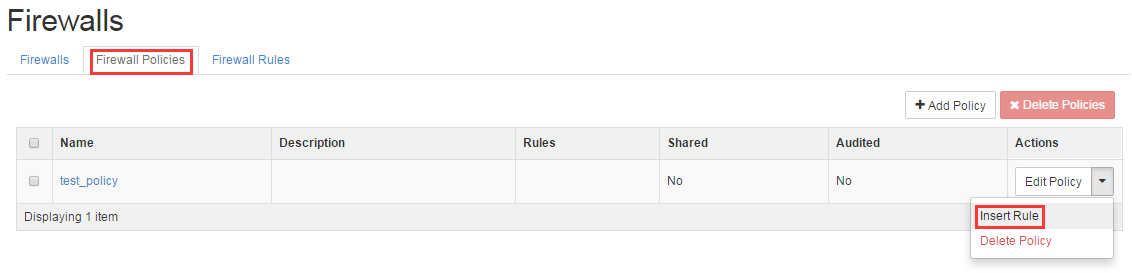


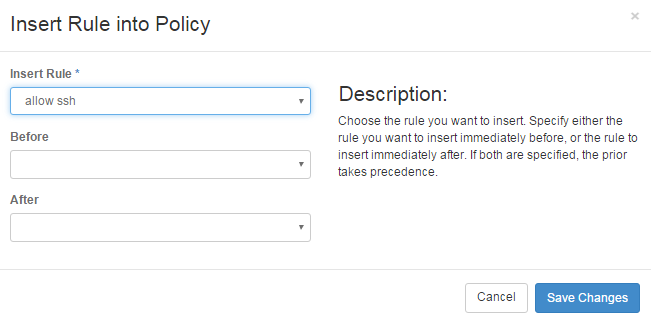
点击 “Add” ，rule 创建成功。



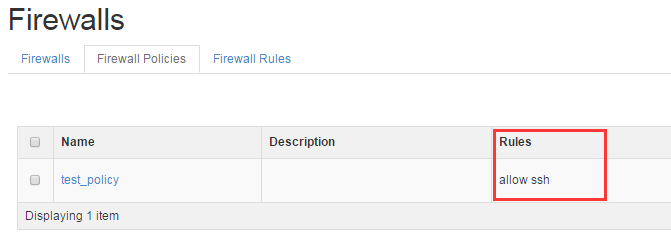
接下来将 rule 添加到 policy 中。

点击 Firewall Policies 标签页面，然后点击 “test\_policy” 后面的 “Insert Rule” 按钮。



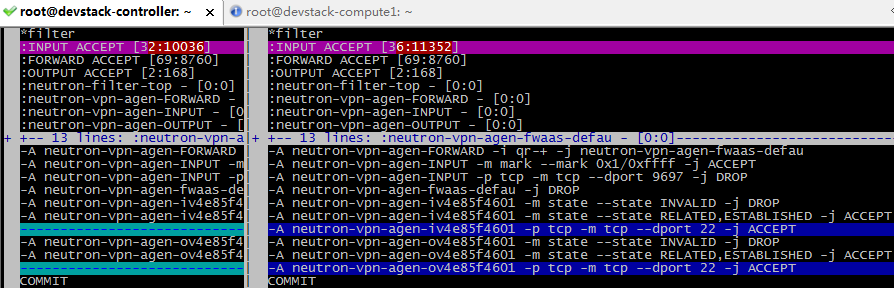


在下拉框中选择 Rule “allow ssh”，点击 “Save Changes”。



可以看到，“allow ssh” 已经成功添加到 “test\_policy” 中。

通过 vimdiff 查看 router namespace 的 iptables-save 发生了什么变化。



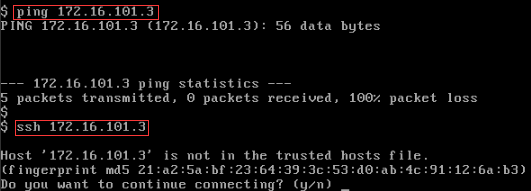
iptables 添加了两条规则：

-A neutron-vpn-agen-iv4e85f4601 -p tcp -m tcp --dport 22 -j ACCEPT

-A neutron-vpn-agen-ov4e85f4601 -p tcp -m tcp --dport 22 -j ACCEPT

其含义是进出 router 的 tcp 数据包，如果目的端口为 22（ssh）ssh，则一律 ACCEPT。

测试一下，cirros-vm1 已经可以 ssh cirros-vm2，但 ping 还是不通，这与预期一致。



“allow ssh” 已经起作用。

同时我们也发现，firewall rule 对进出流量同时生效，不区分方向。

**小节**

FWaaS 用于加强 Neutron 网络的安全性，与安全组可以配合使用。

下面将 FWaaS 和安全组做个比较。

相同点：

1. 底层都是通过 iptables 实现。

不同点：

1. FWaaS 的 iptables 规则应用在 router 上，保护整个租户网络；  
安全组则应用在虚拟网卡上，保护单个 instance。

2. FWaaS 可以定义 allow 或者 deny 规则；安全组只能定义 allow 规则。

3. 目前 FWaaS 规则不能区分进出流量，对双向流量都起作用；  
安全组规则可以区分 ingress 和 egress。

FWaaS 学习完毕，下节我们继续学习 Neutron 的另一个服务 Load Balancing as a Service.