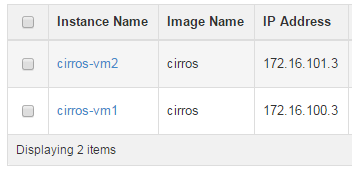
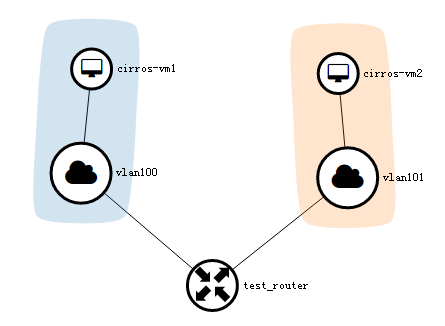


前面我们学习了 FWaaS 的理论知识，今天将通过实验来学习 FWaaS。

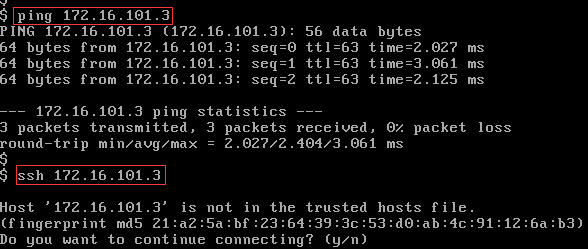
在我们的实验环境中，有两个 instance： cirros-vm1（172.16.100.3） 和 cirros-vm2（172.16.101.3）。



cirros-vm1 和 cirros-vm2 分别位于网络 vlan100 和 vlan101。 vlan100 和 vlan101 之间由虚拟路由器 test\_router 连接。 网络拓扑如下：



在 test\_router 没有应用任何 FWaaS 的情况下，cirros-vm1 可以通过 ping 和 ssh 跨网络访问 cirros-vm2。



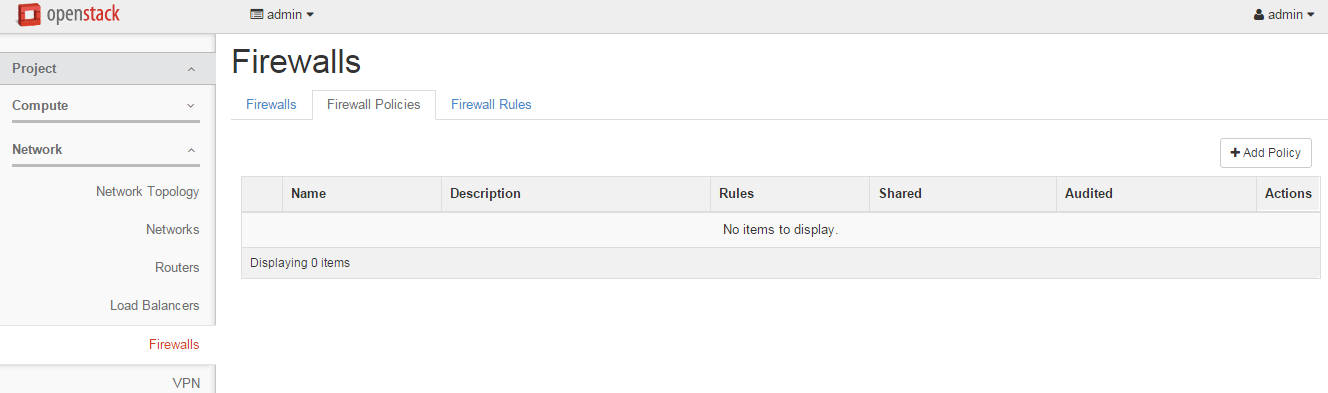
下面我们将进行如下实验： 1. 创建一个不包含任何 rule 的 firewall “test\_firewall” 并应用到 test\_router。  
此时 FWaaS 生效，默认情况下会阻止任何跨子网的流量。

2. 创建 rule 允许 ssh，并将其添加到 test\_firewall。此时 cirros-vm1 应该能够 ssh cirros-vm2。

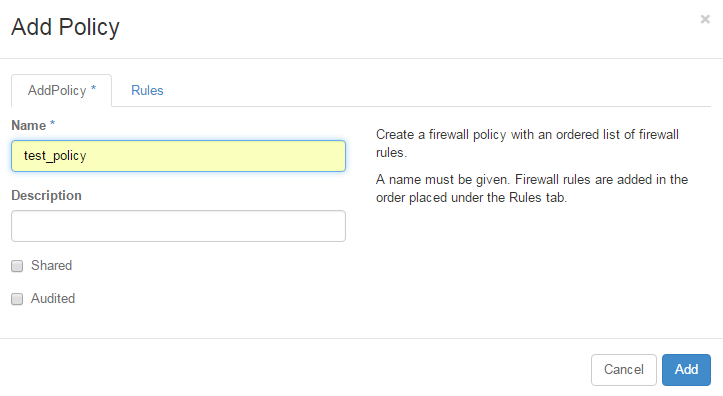
**应用无 rule 的 firewall**

点击菜单 Project -> Network -> Firewalls，打开 Firewall Policies 标签页面。

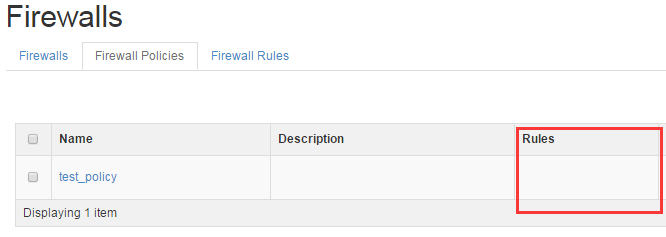
目前没有定义任何 Policie。



点击http://7xo6kd.com1.z0.glb.clouddn.com/upload-ueditor-image-20161127-1480224751947039087.jpg按钮，显示Policy 创建页面。

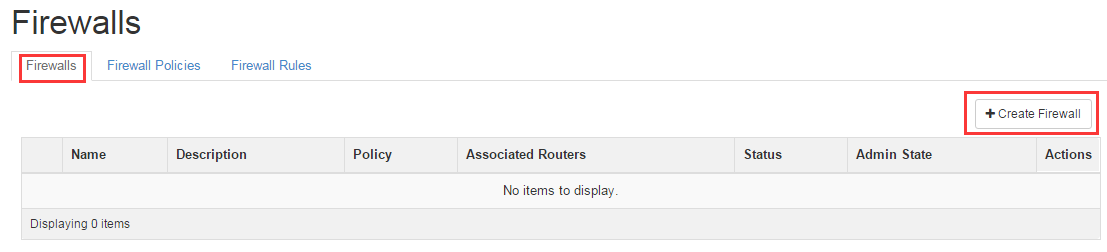


将 Policy 命名为 “test\_policy”，直接点击 “Add” 按钮。

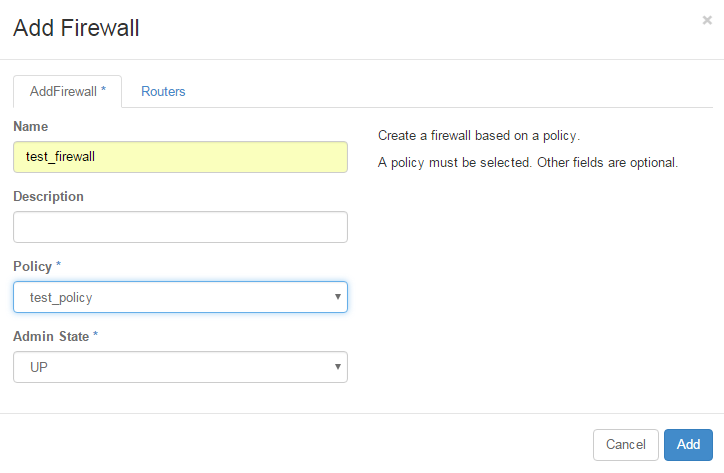


这样我们创建的 test\_policy 不包含任何 Rule。

进入 “Firewalls” 标签页，点击 “Create Firewall” 按钮

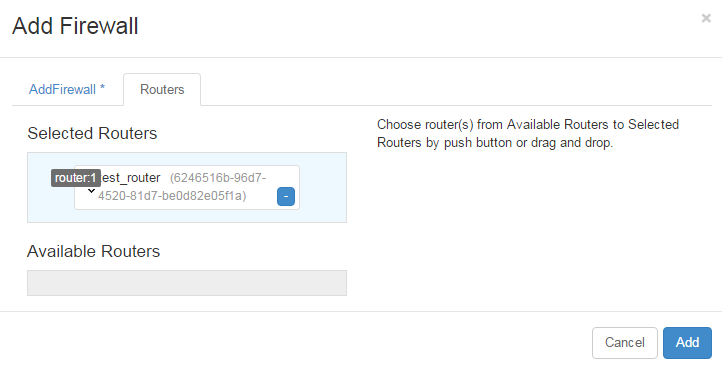


将新的 Firewall 命名为 “test\_firewall”，并关联 “test\_policy”。

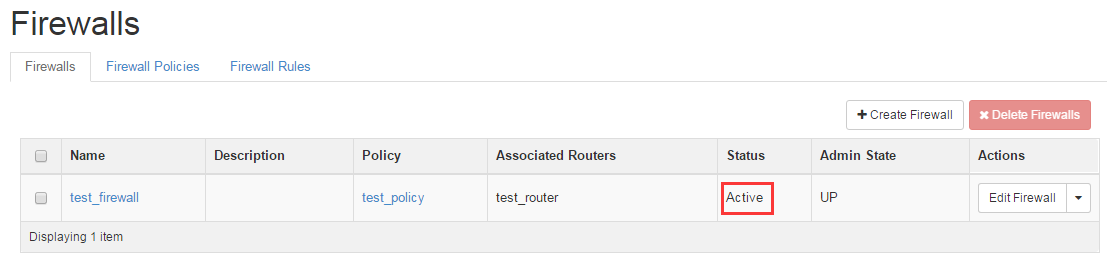


在 “Routers” 标签页中选择 “test\_router”。

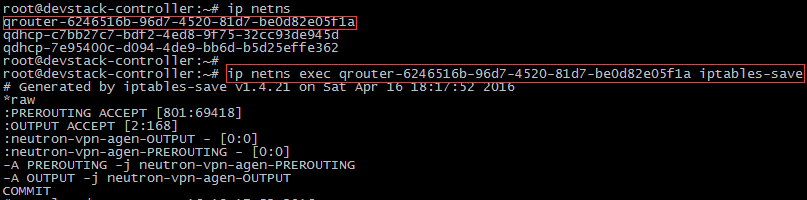
点击 “Add” 创建 firewall。



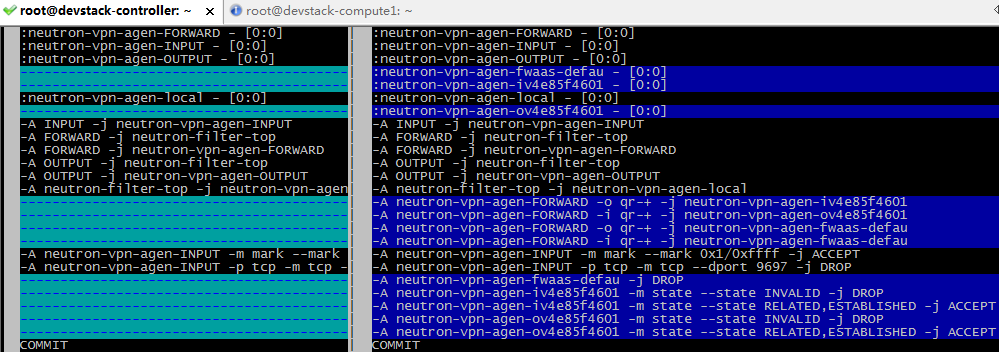
等待 test\_firewall 的 Status 变为 “Active”，此时 test\_router 已经成功应用 test\_policy。



可以通过 iptables-save 查看 router namespace 的 iptables 规则



为了让大家了解底层到底发生了什么变化，下面用 vimdiff 显示了应用 test\_firewall 前后 iptables 规则的变化。



下面我们来分析一下这些规则。

route 在转发数据包时会使用 chain：

-A FORWARD -j neutron-vpn-agen-FORWARD

neutron-vpn-agen-FORWARD 的规则如下：

-A neutron-vpn-agen-FORWARD -o qr-+ -j neutron-vpn-agen-iv4e85f4601

-A neutron-vpn-agen-FORWARD -i qr-+ -j neutron-vpn-agen-ov4e85f4601

-A neutron-vpn-agen-FORWARD -o qr-+ -j neutron-vpn-agen-fwaas-defau

-A neutron-vpn-agen-FORWARD -i qr-+ -j neutron-vpn-agen-fwaas-defau

我们以第一条为例，其含义是：从 router namespace 任何一个 qr-\* interface 发出  
的流量都会应用 chain neutron-vpn-agen-iv4e85f4601，该 chain 定义如下：

-A neutron-vpn-agen-iv4e85f4601 -m state --state INVALID -j DROP

-A neutron-vpn-agen-iv4e85f4601 -m state --state RELATED,ESTABLISHED -j ACCEPT

其规则为：

1. 如果数据包的状态为 INVALID，则 DROP。

2. 如果数据包的状态为 RELATED 或 ESTABLISHED，则 ACCEPT。

其他正常传输的数据怎么处理呢？

回到 neutron-vpn-agen-FORWARD chain 的下一条关于 router 外出数据的规则：

-A neutron-vpn-agen-FORWARD -o qr-+ -j neutron-vpn-agen-fwaas-defau

neutron-vpn-agen-fwaas-defau 内容为：

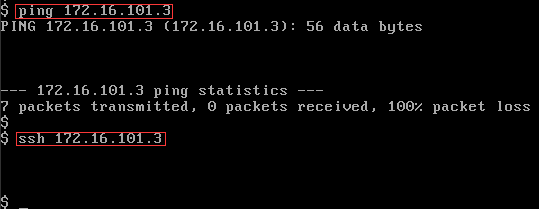
-A neutron-vpn-agen-fwaas-defau -j DROP

可见，数据会被丢弃。

同样的道理，router 上所有进入 qr-\* interface 的数据也会被丢弃。

其结论是：**在没有定义任何 firewall rule 的情况下，进出 router 的数据包都会被丢弃。**

ping 和 ssh 测试表明目前 cirros-vm1 确实已经无法与 cirros-vm2 通信。



下节添加新的规则允许 ssh，之后我们也会比较安全组和 FWaaS 的异同。