



# Cloudos设置安全组为虚拟防火墙固化指导

郑伟 2021-06-29 发表

## 组网及说明

云网融合解决方案标准组网

## 配置步骤

CloudOS安全组的实现方式有三种：交换机流表，CAS ACL，CAS虚拟防火墙。推荐使用CAS虚拟防火墙方式。CloudOS安全组是一个白名单，加入白名单的网段，允许通过，默认为CAS上的ACL策略。

可通过在CAS计算节点容器的/etc/neutron/neutron.conf文件里，设置security\_policy = fw，使用CAS虚拟防火墙以承载安全组功能。修改后，重启openstack-neutron-cas-agent服务，以上配置生效。在计算节点容器中修改配置后需进行相应的固化，否则重启丢失。

- 1、拷贝计算节点容器中的/root/scripts/pre-install.sh至本地
- 2、修改pre-install.sh内容如下

```
if [ $extension_drivers_model != "null" ]; then
openstack-config --set /etc/neutron/plugin.ini ml2 extension_drivers "$extension_drivers_model"
fi

openstack-config --set /etc/neutron/neutron.conf DEFAULT service_plugins h3c_vxplugin_l3_router h3c_l3_router_plugin_h3c3routerPlugin_firewall_base_vpnas
fi

if [ $EXTENSION == "l3" ]; then
cat >> /etc/neutron/neutron.conf <<EOF
[cat]
host_ip = $host_ip
host_username = $username
host_password = $password
security_policy = fw
EOF
fi

if [ $REST_PROTOCOL == "https" ]; then
openstack-config --set /etc/neutron/neutron.conf cas rest_protocol https
fi

INSERT --
```

- 3、执行固化操作指导中的替换脚本完成配置文件替换，容器固化

固化操作请参考《H3C CloudOS5.0镜像固化工具操作指导》相关文档进行

## 配置关键点

附件下载: [Cloudos设置安全组为虚拟防火墙固化指导.doc](#)