CAS 通过ACL策略限制虚拟机网络的典型配置

张月鹏　2020-12-03 发表

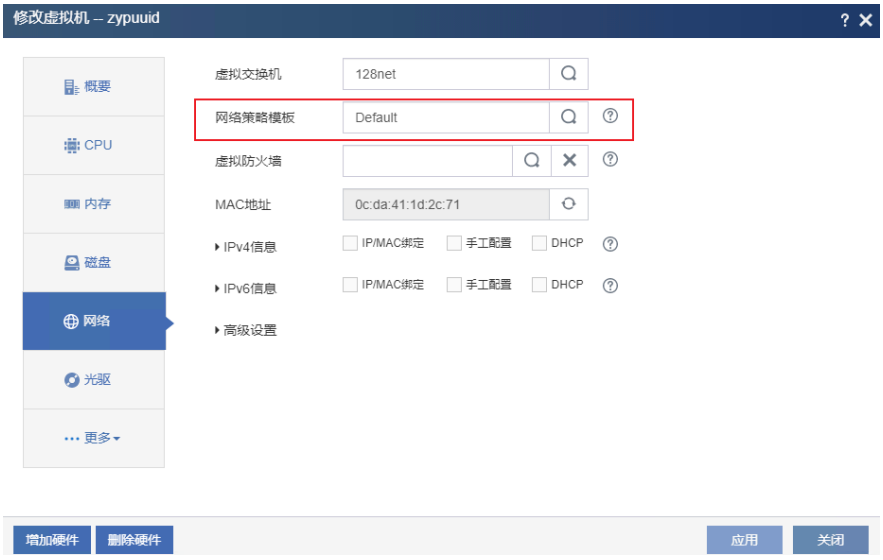
组网及说明

ACL（Access Control List，访问控制列表）是一条或多条规则的集合，用于识别报文流。这里的规则是指描述报文匹配条件的判断语句，匹配条件可以是报文的源IP地址、目的IP地址、端口号等。网络设备依据规则识别出特定的报文，并根据预先设定的策略对流量进行处理。
ACL是一种基于包过滤的安全控制技术。通过ACL可以控制虚拟机之间的网络访问能力，进而保障部署在虚拟机上的业务资源的安全性。
ACL策略管理提供了查看、增加、删除和修改ACL策略及其规则的功能。

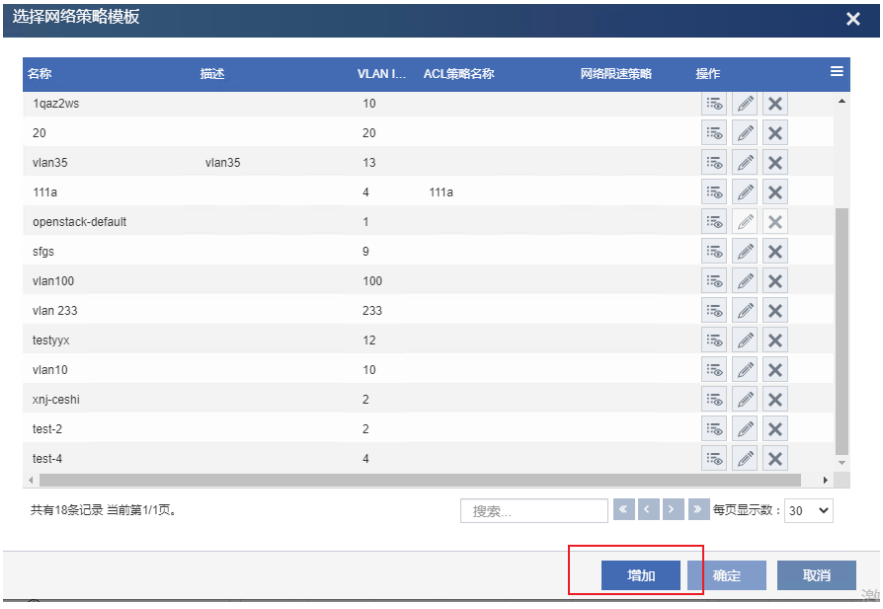
某局点需求虚拟机要求特定网段访问资源，不允许其他网段终端访问。
创建虚拟机192.168.128.205测试，实现需求仅允许127网段访问，不允许其他网段访问（同网段拒绝）

配置步骤

1、修改改虚拟机，新建网络策略模版

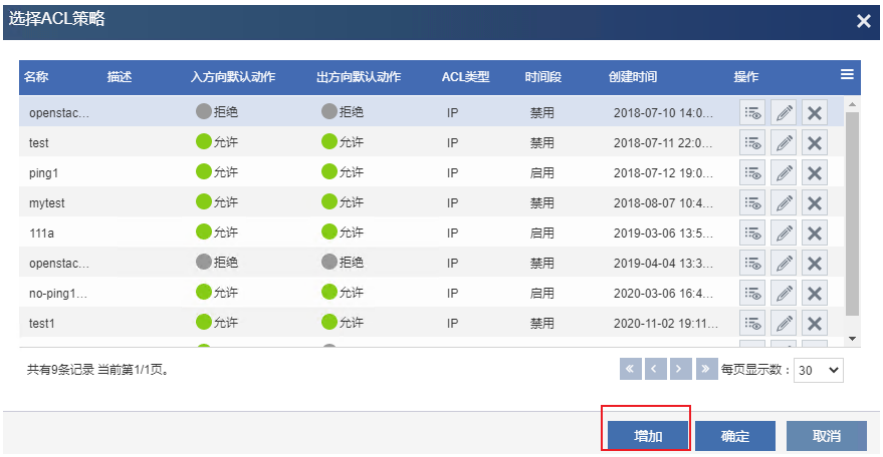


2、增加网络策略模版



3、增加网络策略模版，填写名称，调用ACL策略

4、增加ACL策略配置



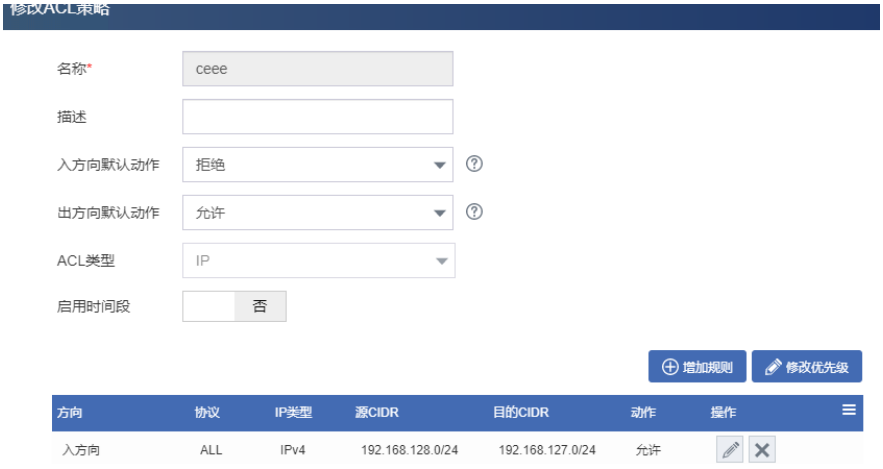
5、通过出、入方向限制均可，如下

配置入方向默认动作为允许，出方向为拒绝，则添加对应网段配置放行规则，注意，ACL策略规则的进出方向是指虚拟交换机的方向，不是虚拟机的方向，即进方向对应于出虚拟机网卡的流量，出方向对应于进虚拟机网卡的流量，

举例，如一台地址为192.168.128.205的虚拟机，仅允许127网段访问，不允许其他网段访问

如配置出方向默认动作为拒绝，即入虚拟网卡vnet方向为拒绝，则配置acl 源地址应配置为127网段，目的地址配置为128。

如配置入方向默认动作为拒绝，即出虚拟网卡vnet方向为拒绝，则配置acl 源地址应配置为128网段，目的地址配置为127。



测试结果如下

测试 192.168.127.32 =>ping 192.168.128.205

测试192.168.128.199=>ping 192.168.128.205

配置关键点

CAS ACL策略规则的进出方向是指虚拟交换机的方向，不是虚拟机的方向，即进方向对应于出虚拟机网卡的流量，出方向对应于进虚拟机网卡的流量；