

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

修改虚拟机 - zypuuid

虚拟交换机: 128net

网络策略模板: Default

虚拟防火墙: []

MAC地址: 0c:da:41:1d:2c:71

IPv4信息: IP/MAC绑定 手工配置 DHCP

IPv6信息: IP/MAC绑定 手工配置 DHCP

高级设置

增加硬件 删除硬件 应用 关闭

2、增加网络策略模版

选择网络策略模板

名称	描述	VLAN ID	ACL策略名称	网络限速策略	操作
1qaz2ws		10			[] [] []
20		20			[] [] []
vlan35	vlan35	13			[] [] []
111a		4	111a		[] [] []
openstack-default		1			[] [] []
sfgs		9			[] [] []
vlan100		100			[] [] []
vlan 233		233			[] [] []
testyxx		12			[] [] []
vlan10		10			[] [] []
xnj-ceshi		2			[] [] []
test-2		2			[] [] []
test-4		4			[] [] []

共有18条记录 当前第1/1页。 搜索... 每页显示数: 30

增加 确定 取消

3、增加网络策略模版, 填写名称, 调用ACL策略

增加网络策略模板

1 基本信息 2 出入口流量设置

名称* test1

描述

ACL策略

VLAN ID* 1

启用网络限速策略 否

下一步

配置详情

名称 test1

描述

ACL策略

VLAN ID 1

增加网络策略模板

1 基本信息 2 出入口流量设置

名称* test01

描述

ACL策略

VLAN ID* 1

启用网络限速策略 否

下一步

配置详情

名称 test01

描述

ACL策略

VLAN ID 1

4、增加ACL策略配置

选择ACL策略

名称	描述	入方向默认动作	出方向默认动作	ACL类型	时间段	创建时间	操作
openstac...		拒绝	拒绝	IP	禁用	2018-07-10 14:0...	
test		允许	允许	IP	禁用	2018-07-11 22:0...	
ping1		允许	允许	IP	启用	2018-07-12 19:0...	
mytest		允许	允许	IP	禁用	2018-08-07 10:4...	
111a		允许	允许	IP	启用	2019-03-06 13:5...	
openstac...		拒绝	拒绝	IP	禁用	2019-04-04 13:3...	
no-ping1...		允许	允许	IP	启用	2020-03-06 16:4...	
test1		允许	允许	IP	禁用	2020-11-02 19:11...	

共有9条记录 当前第1/1页。

增加 确定 取消

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。

名称* ceee

描述

入方向默认动作 允许 ?

出方向默认动作 拒绝 ?

ACL类型 IP

启用时间段 否

+ 增加规则 修改优先级

方向	协议	IP类型	源CIDR	目的CIDR	动作	操作
出方向	ALL	IPv4	192.168.127.0/24	192.168.128.0/24	允许	

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。

修改ACL策略

名称* ceee

描述

入方向默认动作 拒绝 ?

出方向默认动作 允许 ?

ACL类型 IP

启用时间段 否

+ 增加规则 修改优先级

方向	协议	IP类型	源CIDR	目的CIDR	动作	操作
入方向	ALL	IPv4	192.168.128.0/24	192.168.127.0/24	允许	

测试结果如下

测试 192.168.127.32 => ping 192.168.128.205

```
C:\Users\test>ping 192.168.128.205
正在 Ping 192.168.128.205 具有 32 字节的数据:
来自 192.168.128.205 的回复: 字节=32 时间=1ms TTL=127
来自 192.168.128.205 的回复: 字节=32 时间=1ms TTL=127
来自 192.168.128.205 的回复: 字节=32 时间=1ms TTL=127
来自 192.168.128.205 的回复: 字节=32 时间=18ms TTL=127
```

测试 192.168.128.199 => ping 192.168.128.205

```
C:\Users\Administrator>ping 192.168.128.205
正在 Ping 192.168.128.205 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。
```

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；