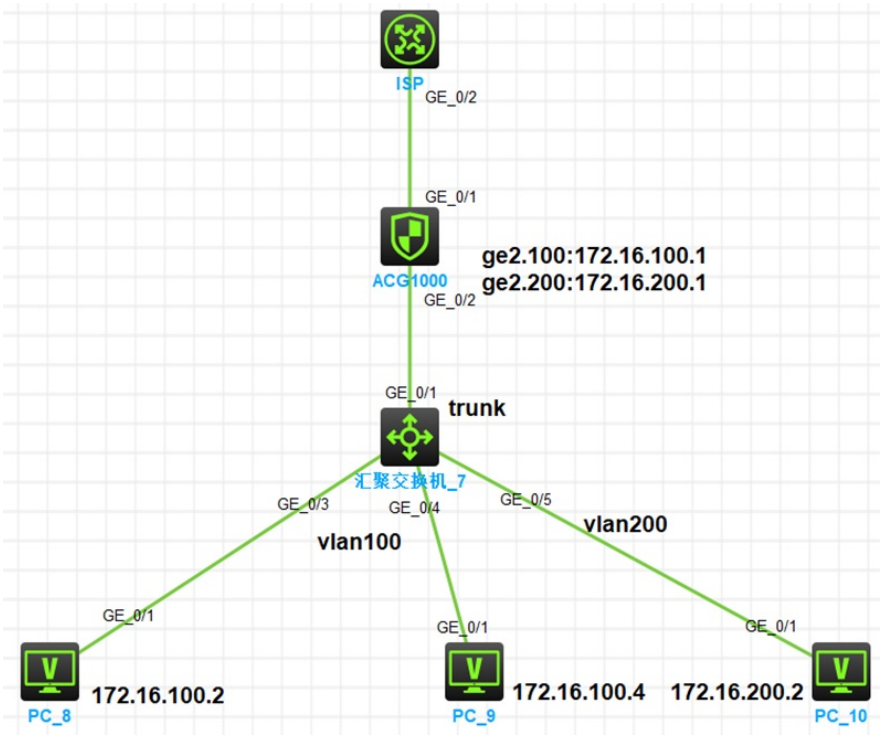
ACG1000实现部分网段仅IP+mac绑定的终端可以上网(ACG作为网关)

ACG1000 薛佳宇 2023-03-11 发表

组网及说明

一、拓扑



二、需求

内网网关ACG1000设备，要求内网网段vlan100:172.16.100.0/24的终端只有在ACG上完成IP+MAC绑定后才能上网。内网vlan 200:172.16.200.0/24网段不做限制。

三、配置思路

1、ACG作为网关则可以直接学习到终端的真实mac地址，可以直接在设备上手工增加IP+MAC绑定表项，添加时开启唯一性。

2、ACG默认控制策略为允许，需要在ACG上配置控制策略：①允许源地址是vlan100permit即172.16.100.0/24中允许上网的地址的流量；②禁止源地址是vlan100即172.16.100.0/24的流量；③允许源地址是vlan200即172.16.200.0/24的流量(可不配，因为默认动作为允许)

3、需要新增可以上网的pc时需要：①、在IP+MAC绑定的位置增加IP和MAC的绑定信息，并开启唯一性；②、在允许vlan100上网的地址对象组中添加允许的ip

配置步骤

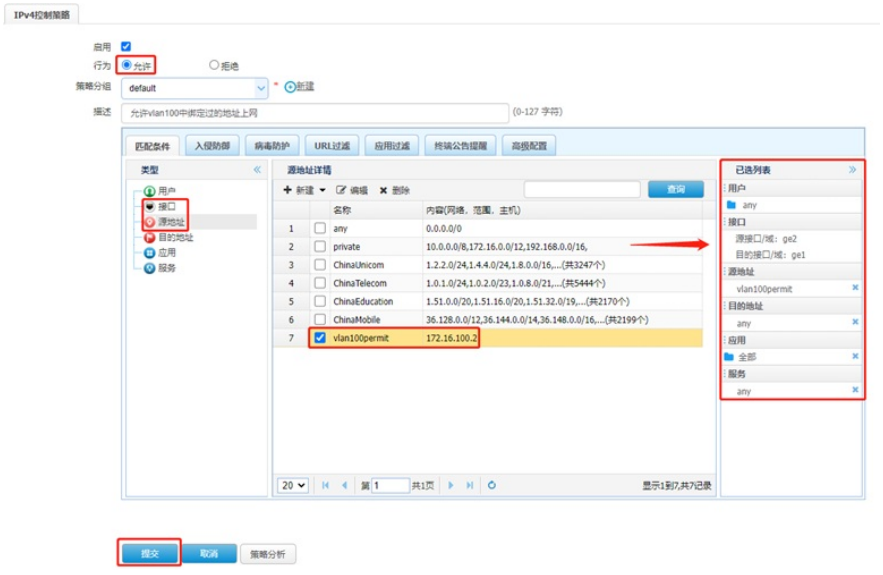
四、配置步骤

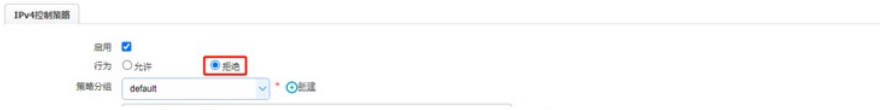
1、配置地址对象组vlan100permit包含vlan100中可以上网的地址，地址对象组vlan100包含整个vlan100的网段。、

1、ACG作为网关可以直接学习到终端真实mac地址，所以不用配置SNMP同步(跨三层mac学习)

2、配置IP-MAC绑定时要开启唯一性

2、配置控制策略，第一条仅允许vlan100permit地址组中的地址上网，第二条禁止所有vlan100地址对象组中地址上网。第三条可以新建允许其他地址上网，也可以配置控制策略默认动作为允许。控制策略按照从上往下的顺序匹配。




IPv4控制策略
启用
行为
允许
拒绝
策略分组
default
新建