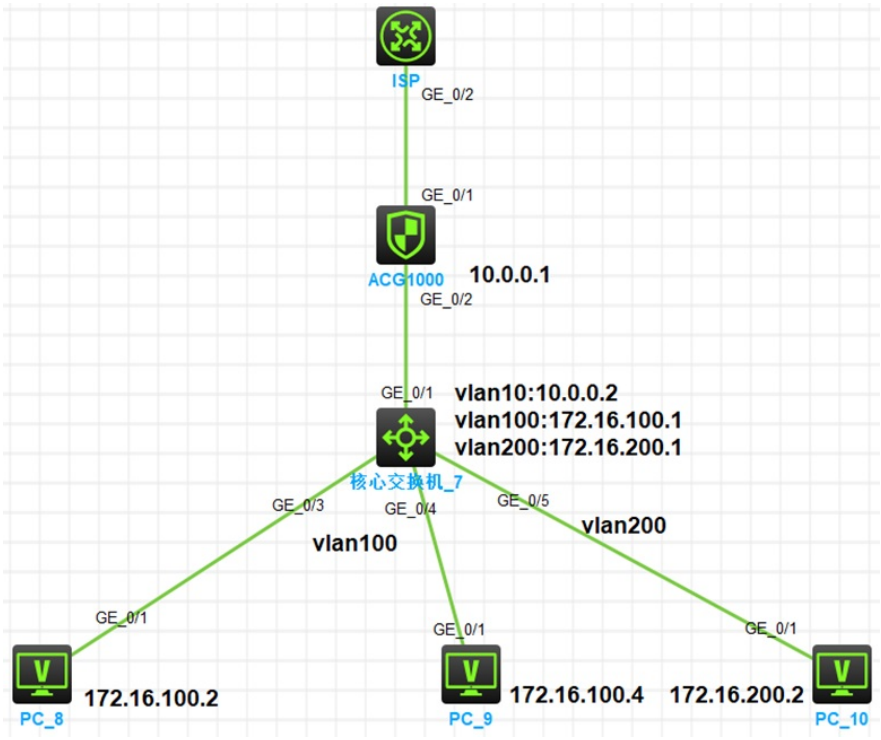
ACG1000实现部分终端禁止访问部分网站(ACG在网关上层)

ACG1000 薛佳宇 2023-03-11 发表

组网及说明

一、拓扑



二、需求

内网网关在核心交换机，ACG1000设备作为出口。要求内网网段vlan100中终端PC1 172.16.100.4(8c-16-45-5d-88-e6)不能访问淘宝和斗鱼，其他网站不做限制，其他终端不做限制。

三、配置思路

(1)方法一：使用终端mac地址控制

1、ACG设备在终端网关设备上层，因此默认情况下ACG1000设备无法学习到终端的真实mac地址，如果需要通过mac地址来控制则需要在ACG上配置SNMP同步(跨三层mac学习)。

2、为了配合ACG设备完成SNMP同步，需要在核心交换机配置SNMP。

3、acg创建本地用户，绑定终端真实mac地址8c-16-45-5d-88-e6

4、配置URL对象组，包含禁止访问的域名

5、配置IPV4控制策略，匹配上述用户，通过URL过滤模块进行控制，其他终端可配置控制策略放行，或配置控制策略默认动作为允许

(2)方法二：使用终端ip地址控制(可以不配置SNMP同步)

1、配置URL对象组，包含禁止访问的域名

2、配置IPV4控制策略，源地址匹配包含要限制的IP的IP地址对象组，通过URL过滤模块进行控制，其他终端可配置控制策略放行，或配置控制策略默认动作为允许

配置步骤

四、配置步骤

(1) 方法一：使用终端mac地址控制

1、核心交换机配置基础网络及SNMP，ACG配置基础网络。仅列举交换机snmp配置：

```
#
snmp-agent
snmp-agent community read acg
snmp-agent sys-info version all
#
```

2、ACG设备配置SNMP同步

3、ACG针对上述终端添加本地用户，名为url控制，绑定终端mac地址

1、ACG设备在终端网关设备上层，因此默认情况下ACG1000设备无法学习到终端的真实mac地址，如果需要通过mac地址来控制则需要在ACG上配置SNMP同步(跨三层mac学习)。

2、配置SNMP同步时，填写的mac地址是交换机与ACG互联的三层接口的mac，也就是本案例中vlan-int的mac

4、配置URL对象组，包含禁止访问的域名

5、ACG设备配置控制策略，匹配条件中选中用户"URL限制"，随后URL过滤模块中创建一条规则：访问"禁止的网站"为拒绝。


H3C
SecPath ACG1000
主页
数据中心
策略配置
用户管理
网络配置
系统管理
策略配置
IPv4审计策略
IPv4控制策略
策略分析
新建
删除
查询
启用
禁用
优先级
匹配次数清零
默认规则
允许
拒绝