ACG1000产品单臂路由模式部署方法

设备部署方式 张旭 2019-04-08 发表

组网及说明

1 配置需求或说明

1.1 适用的产品系列

本案例适用于软件平台为ACG1000系列应用控制网关：ACG10X0、ACG1000-AKXXX等。

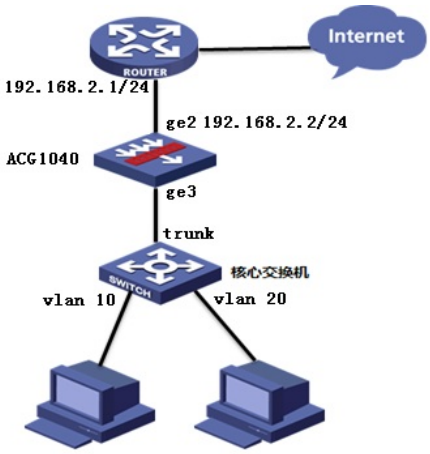
注：本案例是在ACG1040的Version 1.10, Release 6609P06版本上进行配置和验证的。

1.2 配置需求及实现的效果

如下图所示，需要在原有的网络中增加ACG1040来审计内网用户上网行为，为了让不同网段用户互访流量也能通过进行审计，需要将内网各网段网关上移配置在ACG1040上；其中ge2接口接原有路由器的下联口，ge3接口接原有的交换机上联口。

2 组网图

组网介绍：核心交换机通过一条线路连接至ACG1040 ge3端口，交换机Vlan 10网关为192.168.10.1/24、Vlan 20网关为192.168.20.1/24，需要ACG可以终结Vlan10与Vlan 2的vlan标签，并审计用户上网行为。



配置步骤

3 配置步骤

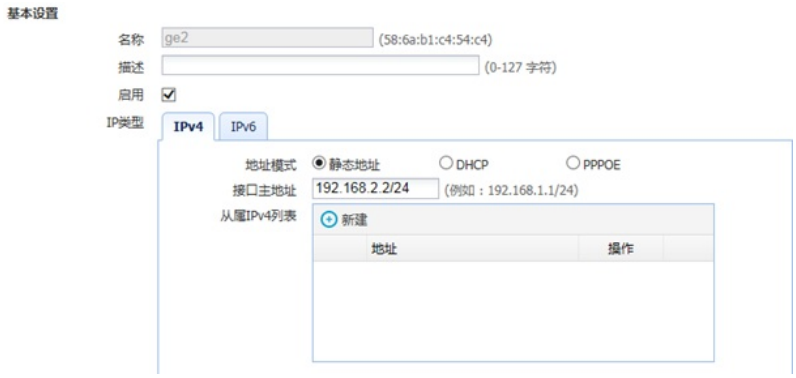
3.1 登录设备管理界面

设备管理口（ge0）的默认地址配置为192.168.1.1/24。默认允许对该接口进行PING，HTTPS操作。将终端与设备ge0端口互联，在终端打开浏览器输入https://192.168.1.1登录设备管理界面。默认用户名与密码均为admin。

3.2 配置连接路由器接口

#选择“网络配置”>“接口”>“物理接口”中点击ge2接口后的编辑按钮，进行端口修改。

#设置ge2接口IP地址为192.168.2.2/24。



#在接口选项下的“高级设置”>“接口属性”中将ge2接口设置为外网接口。

3.3 配置连接核心交换机接口

#选择“网络配置”>“接口”>“子接口”中新建子接口。

3.3.1 创建Vlan 10虚接口并配置地址

#名称选择ge3并在主接口后添加Vlan ID 10，配置接口IP地址为192.168.10.1/24。

3.3.2 创建Vlan 20虚接口并配置地址

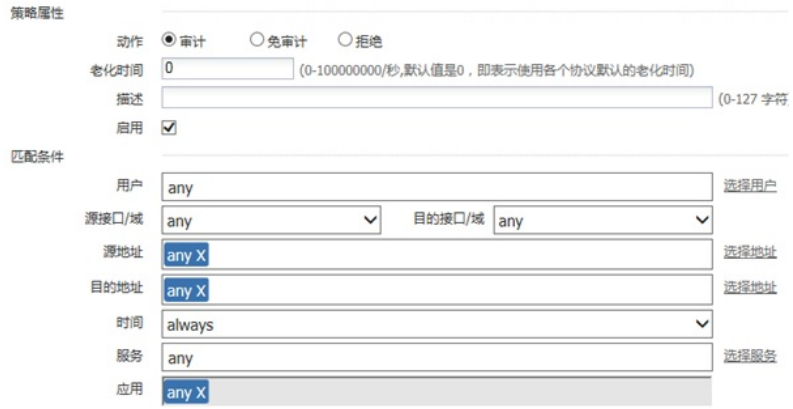
#名称选择ge3并在主接口后添加Vlan ID 20，配置接口IP地址为192.168.20.1/24。

3.4 配置路由

#选择“网络配置”>“路由”>“静态路由”>“新建”中创建静态路由。目的地址和掩码都设置为：0.0.0.0（代表所有网段），下一跳地址配置192.168.2.1（路由器下联接口地址），配置完成后点击提交。

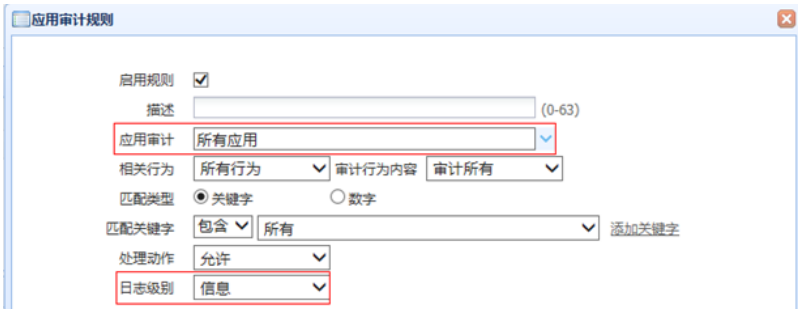
3.5 配置IPV4策略审计用户流量

#选择“上网行为管理”>“策略配置”>“IPV4策略”>“新建”中创建审计策略。



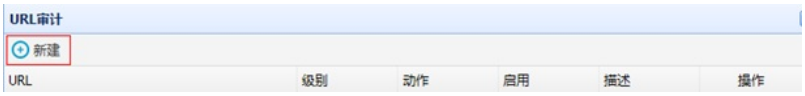
注：下图中各参数使用默认配置即可。

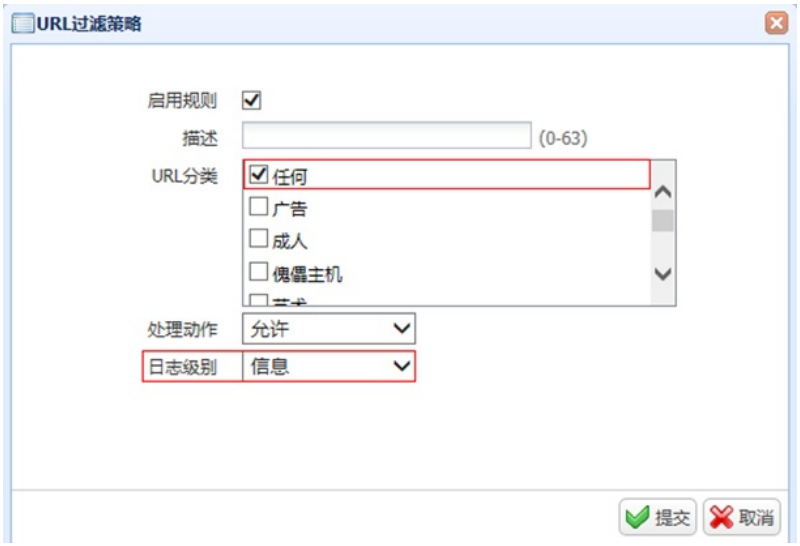
新建应用审计策略用来审计所有应用。



注：这里的日志级别需要设置为信息，否则设备不记录日志。

新建URL审计策略审计所有网站，配置完成后选择提交完成所有配置。





3.6 配置保存

#在设备管理界面右上角点击配置保存，保存当前配置。

3.7 交换机配置

#连接ACG接口配置

interface GigabitEthernet 1/0/1

port link-type trunk

port trunk permit vlan all

#连接vlan 10主机接口配置

interface GigabitEthernet 1/0/10

port access vlan 10

#连接vlan 20主机接口配置

interface GigabitEthernet 1/0/20

port access vlan 20

3.8 策略验证

用户网站访问“中国搜索”、“51cto”等网站测试：

#在“日志查询”>“网站访问日志”>“访问网站日志”中查看对应日志。

#在“日志查询”>“应用审计日志”>“搜索引擎日志”中查看对应日志。

配置关键点

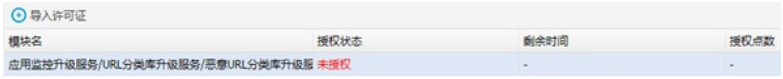
3.9 注意事项

1、 目前ACG1000默认情况下只能过滤HTTP网页，如果遇到HTTPS网页如百度、淘宝、京东等需要配置HTTPS解密策略，才能正常过滤。

注：HTTPS解密策略需要升级ACG版本至R6608以上版本才能支持。

2、 应用审计功能需要购买特征库激活文件并激活后才能使用，如果特征库授权未激活或者特征库授权过期则无法保证应用审计功能正常使用。

#在“系统管理”>“授权管理”中可查看授权是否为已授权状态。



注：出现上图中“未授权”字样则表示没有授权，无法使用应用识别功能。