ACG1000产品旁路模式部署方法

旁路部署 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。

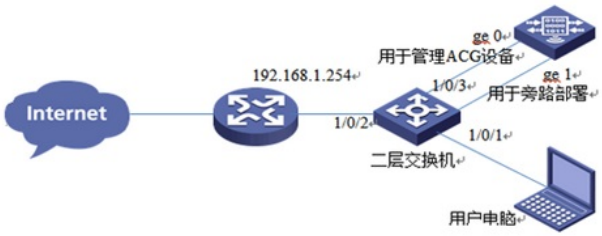
注：本案例是在ACG1040的Version 1.10, Release 6609P06版本上进行配置和验证的。

1.2 配置需求及实现的效果

如下组网图所示，需要在原有的网络中增加ACG1040来审计内网用户上网行为，为最小程度避免影响原有网络，所以ACG1040采用旁路模式部署进原有网络；

2 组网图

组网说明：ACG1040旁路部署连接在二层交换机1/0/1接口，因为用户需要有通过网络访问ACG的需求，所以需要再连一条网线到交换机用于跨网段管理ACG使用。



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 配置旁路接口

#选择“系统管理”>“部署方式”>“旁路部署”中勾选ge1接口，在弹出的对话框中选择“确定”。

3.3 配置管理接口

#选择“网络配置”>“接口”>“物理接口”中将ge0接口IP地址修改为192.168.1.11/24。

注：修改完成后与ACG管理界面断开，需要将管理电脑连入交换机后使用https://192.168.1.11重新登录ACG1040进行管理。

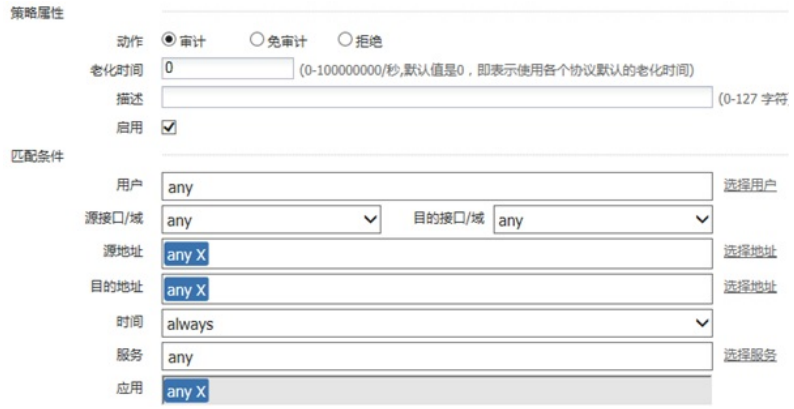
3.4 配置路由

#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192.168.1.254（路由器下联接口地址），配置完成后点击提交。

注：这不操作是保证ACG可以被其他网段终端管理。

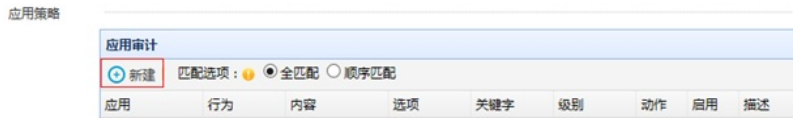
3.5 配置IPV4策略审计用户流量

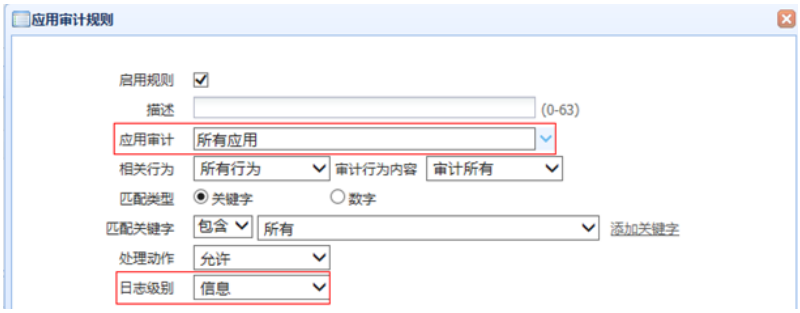
#选择“上网行为管理”>“策略配置”>“IPV4策略”>“新建”中创建审计策略。



注：下图中各参数使用默认配置即可。

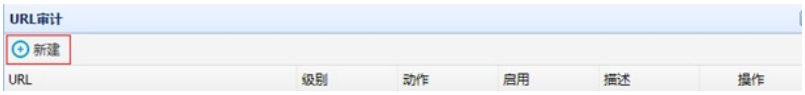
新建应用审计策略用来审计所有应用。

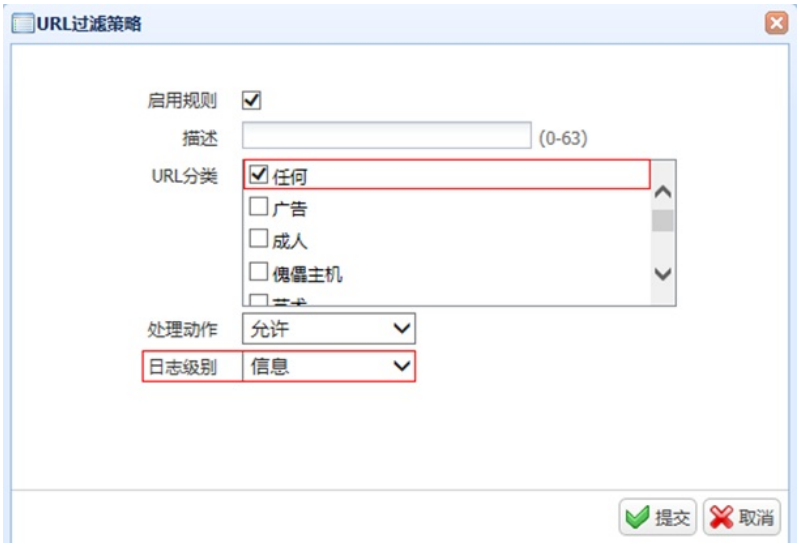




注：这里的日志级别需要设置为信息，否则设备不记录日志。

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 交换机端口镜像

因为旁路模式中数据流量无法通过ACG，所以需要借助交换机端口镜像功能，将通过交换机的流量复制一份送上ACG进行审计。

H3C交换机配置：

```
#配置本地端口镜像
mirroring-group 1 local
#配置1/0/2为镜像端口(交换机上联端口)
interface Ethernet1/0/2
 loopback-detection enable
 mirroring-group 1 monitor-port
#设置1/0/3为被镜像端口（连接ACG端口）
interface Ethernet1/0/3
 loopback-detection enable
 mirroring-group 1 mirroring-port both
```

注：不同厂商交换机复制端口流量有不同的方法，详询对应交换机产商售后。

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

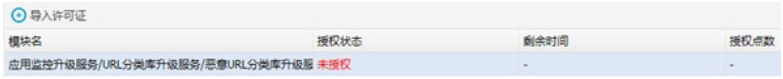
3.9 注意事项

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。

3、 旁路模式部署后只能对用户流量进行审计，无法做到对用户流量进行阻断等操作。