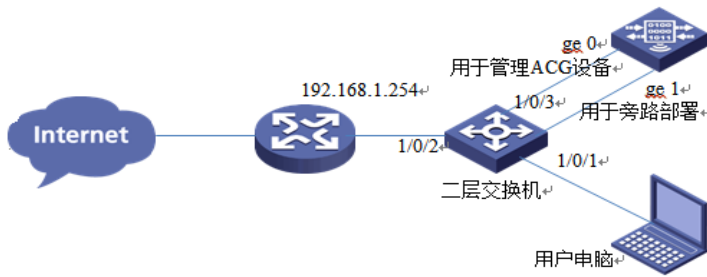


为了不影响源网络拓扑的情况下，实现对内网数据的审计和监控。



1) 旁路模式设置

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



2) 配置管理接口

配置管理接口使管理员能从内网访问ACG1040，对监控内容进行审计。



注：因为选择接口为旁路模式后接口默工作在二层模式下，所以需在其它接口上配置管理ip。

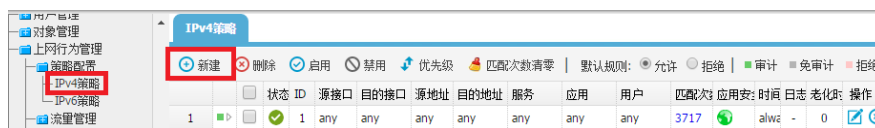
3) 添加路由

添加一条到内网网关的路由用作其它内网网段管理。



4) 添加IPv4策略

上网行为>策略配置>IPv4配置>新建IPv4策略



5) 新建匹配条件

策略属性

动作 审计 免审计 拒绝

老化时间 (0-1728000/秒, 默认值是0, 即表示使用各个协议默认的老化时间)

启用

匹配条件

用户 选择用户

源接口/域 目的接口/域

源地址 选择地址

目的地址 选择地址

时间

服务 选择服务

应用

6) 新建应用审计策略

应用审计规则

启用规则

描述 (0-127)

应用审计

相关行为 审计行为内容

匹配类型 关键字 数字

匹配关键字 添加关键字

处理动作

日志级别

7) 如果有需求新建URL过滤策略

URL过滤策略

启用规则

描述 (0-63)

URL分类

- 任何
- 广告
- 成人
- 傀儡主机

处理动作

日志级别

注: 这里的日志级别一定需要设置, 否则不会有日志输出。

8) 配置引流需要将流量引上ACG

应用审计

新建 删除 | 匹配选项: 全匹配 顺序匹配

应用	行为	内容	选项	关键字	级别	动作	启用	描述	操作
1	百度	所有行为	所有行为内容包含	any	通知	允许	<input checked="" type="checkbox"/>	-	<input type="button" value="编辑"/> <input type="button" value="删除"/>
2	百度贴吧	所有行为	所有行为内容包含	any	不记录	允许	<input checked="" type="checkbox"/>	-	<input type="button" value="编辑"/> <input type="button" value="删除"/>

20 | 第 1 页 | 共 1 页 | 当前显示 1 到 2, 共 2 记录

URL审计

新建 删除

URL	级别	动作	启用	描述	操作	
1	any	信息	允许	<input checked="" type="checkbox"/>	-	<input type="button" value="编辑"/> <input type="button" value="删除"/>

20 | 第 1 页 | 共 1 页 | 当前显示 1 到 1, 共 1 记录

交换机上的配置

```

mirroring-group 1 local //配置本地端口镜像
#
interface Ethernet1/0/2 //配置0/2为镜像端口
loopback-detection enable
mirroring-group 1 monitor-port
#
interface Ethernet1/0/3 //设置0/3为被镜像端口
loopback-detection enable
mirroring-group 1 mirroring-port both

```

配置关键点:

- 1、选择为旁挂的端口是不能配置ip进行管理设备的, 想要管理设备需要在设备上找一个接口配置ip地

址和网络相连接。

2、网站URL审计只能对于HTTP报文进行审计无法对HTTPS进行审计，这个并非我司设备问题。HTTPS报文在传输的过程中是通过加密的。无法从报文头中提取索引。

3、用户日志无法出现时请确认，1、特征库是否为最新版本。2、IPV4策略中是否选择了日志级别。3、到底是不是具体的应用在访问还是用URL去访问测试的。