

组网及说明

1 配置需求或说明

1.1 适用的产品系列

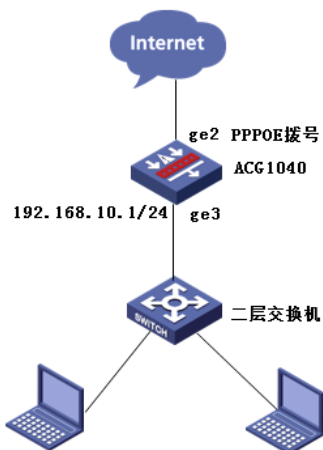
本案例适用于软件平台为ACG1000系列应用控制网关：ACG10X0、ACG1000-AKXXX等。

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，将ACG1040部署在外网出口作为路由器使用，外网使用PPPOE拨号方式上网，同时需要ACG1040为内网用户下发IP地址提供互联网接入。其中ge2接口连接外网，ge3接口连接内网二层交换机。

2 组网图



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 配置连接互联网接口

#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。

物理接口	子接口	网桥接口	聚合接口	隧道接口	无线接口	安全域				
接口名称	描述	IP地址	IPv6地址	MAC地址	工作模式	双工模式	速率(Mbps)	连接状态	启用状态	操作
1	ge0	192.168.1.1/24		58-6a-b1-c4-5	route	full	1000	up	<input checked="" type="checkbox"/>	
2	ge1			58-6a-b1-c4-5	route	full	1000	down	<input checked="" type="checkbox"/>	
3	ge2			58-6a-b1-c4-5	route	full	1000	up	<input checked="" type="checkbox"/>	
4	ge3			58-6a-b1-c4-5	route	full	1000	up	<input checked="" type="checkbox"/>	

#设置ge2地址模式为PPPOE并填入运营商提供的上网账号和密码，PPPOE属性中必须勾选“更新网关”和“更新DNS”。

网络接口

基本设置

名称 (58:6a:b1:c4:54:c4)

描述 (0-127 字符)

启用

IP类型 **IPv4** IPv6

地址模式 静态地址 DHCP PPPoE

PPPoE

接口主地址 -

用户名 (1-255)

密码 (1-31)

优先级 (1-255)

PPPoE属性 更新网关 更新DNS

#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，设置完成后点击提交。

高级配置

协商模式 自动 强制

MTU (1280-1500)

接口属性 内网口 外网口

提交

取消

配置完成后在“系统监控”>“接口状态”中查看ge2端口是否获取了IP地址，如果无法获取IP地址请联系运营商确认账号密码是否正确？

接口状态

清除计数

名称	链路状态	属性	工作速	双工模	IP地址	IPv6地址	接收速率	发送速率	接收总包数	接收总字节数	发送总包数	发送总字节数	MAC地址
1	ge0	up	-	1000	full	192.168.1.1/24	147.61 Kbps	6.05 Mbps	114950	12901539	265146	346826745	58-6a-b1:c4-54:c
2	ge1	-	-	1000	full		0 bps	0 bps	0	0	0	0	58-6a-b1:c4-54:c
3	ge2	up	pppoe	1000	full	198.76.28.2/32	0 bps	0 bps	19971	16200845	23468	2847344	58-6a-b1:c4-54:c
4	ge3	up	-	1000	full		510 bps	0 bps	35145	4121109	33156	33702626	58-6a-b1:c4-54:c

3.3 配置Snat地址转换

#选择“网络配置”>“NAT”>“源NAT”点击新建。

接口位置选择ge2（连接外网接口）后点击提交。

源NAT规则

源地址

目的地址

服务

接口

转换类型 出接口 地址池 不转换

日志

提交 取消

3.4 配置连接核心交换机接口

#选择“网络配置”>“接口”>“物理接口”中点击ge3接口后的编辑按钮，进行端口修改。

物理接口	子接口	网络接口	聚合接口	隧道接口	无线接口	安全域				
接口名称	描述	IP地址	IPv6地址	MAC地址	工作模式	双工模式	速率(Mbps)	连接状态	启用状态	操作
1	ge0	192.168.1.1/24		58-6a-b1:c4-54:c	route	full	1000	up	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	ge1			58-6a-b1:c4-54:c	route	full	1000	down	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	ge2	198.76.28.2/32		58-6a-b1:c4-54:c	route	full	1000	up	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	ge3			58-6a-b1:c4-54:c	route	full	1000	up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

设置ge3接口IP地址为192.168.10.1/24。

网络接口

基本设置

名称 (58:6a:b1:c4:54:c5)

描述 (0-127 字符)

应用

IP类型 **IPv4** IPv6

地址模式 静态地址 DHCP PPPOE

接口主地址 (例如: 192.168.1.1/24)

从属IPv4列表

<input checked="" type="radio"/> 新建	
地址	操作

#在接口选项下的“高级设置”>“接口属性”中将ge3接口设置为内网接口。

高级配置

协商模式 自动 强制

MTU (1280-1500)

接口属性 内网口 外网口

3.5 配置DHCP为内网用户分发地址

#选择“网络配置”>“DHCP服务器”>“DHCP服务”中ge3接口DHCP服务开启。

接口	服务	中继服务器地址	操作
1 ge0	无		<input checked="" type="checkbox"/>
2 ge1	无		<input checked="" type="checkbox"/>
3 ge2	无		<input checked="" type="checkbox"/>
4 ge3	无		<input checked="" type="checkbox"/>

将 ge3接口设置为DHCP服务器

DHCP服务

接口名称

服务类型 空 DHCP中继代理 DHCP服务器

#选择“网络配置”>“DHCP服务器”>“地址池”中新建DHCP地址池中，完成下面配置：

DHCP服务 **服务器** **排除范围** **IP-MAC绑定** **监视器**

名称	地址池

DHCP列表

基本设置

名称 (1-31 字符)

子网/掩码

网关 (与所选接口匹配)

IP地址开始

IP地址结束

租约 无限 有限期

时间 天 小时 分钟 (5 分钟-100 天)

高级配置

DNS1

DNS2

Wins1

Wins2

域

AC1

AC2

注：子网掩码需要添加下发网段的网络位地址（一般子网的网络位最后一位为0），网关地址填写ge3接口地址，租约时间建议设置为24小时，否则会造成IP地址分配后无法回收。DNS地址填写运营商提供的DNS地址，如果没有提供请填写114.114.114.114或者8.8.8.8作为DNS服务器。

3.6 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。

策略属性

动作 审计 免审计 拒绝

老化时间 (0-100000000/秒,默认值是0,即表示使用各个协议默认的老化时间)

描述 (0-127 字符)

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

新建应用审计策略用来审计所有应用。

应用策略

应用审计

新建 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
----	----	----	----	-----	----	----	----	----

应用审计规则

启用规则

描述 (0-63)

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

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。

URL审计

新建

URL	级别	动作	启用	描述	操作
-----	----	----	----	----	----

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

3.7 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。



3.8 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。



网站访问日志

查询 导出 查询结果：在 2019-01-26 的 5 条日志记录中，从 1 - 5 搜索出相关结果 5 条，显示 1 - 20

用户	用户IP	URL分类	网页标题	URL	处理动作	级别	时间
1	192.168.10.88	48:0f:c1:27:79:24	其他	中国搜索-国家权威搜索引擎	放行	信息	2019-01-26 17:28:05
2	192.168.10.88	48:0f:c1:27:79:24	其他	51CTO.COM - 技术成就梦想 - 中国领先的IT技术网	放行	信息	2019-01-26 17:27:44

#在“日志查询”>“应用审计日志”>“搜索引擎日志”中查看对应日志。

搜索引擎日志

查询 导出 查询结果：在 2019-01-26 的 2 条日志记录中，从 1 - 2 搜索出相关结果 2 条，显示 1 - 20

用户	用户IP	应用	行为	处理动作	内容	系统	终端	级别	时间	
1	192.168.10.88	48:0f:c1:27:79:24	中国搜索	Q、搜索	放行	360	Windows	PC	信息	2019-01-26 17:31

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HTPS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。

导入许可证

模块名	授权状态	剩余时间	授权点数
应用监控升级服务/URL分类库升级服务/恶意URL分类库升级服	未授权	-	-

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。

配置关键点