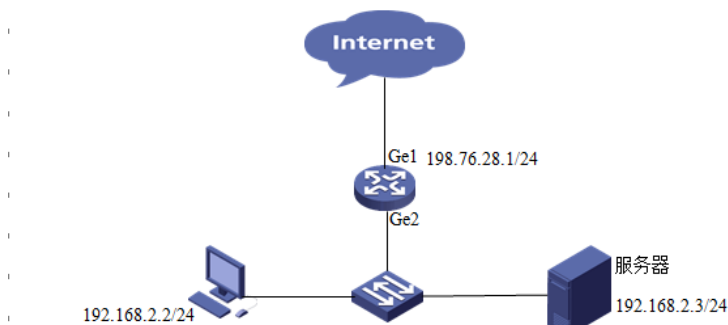


知 ACG1000系列设备实现内网电脑通过公网地址访问内部服务器

ACG1000 NAT 刘嘉炜 2016-03-19 发表

某局点使用ACG1040作为外网出口设备，想要实现内网用户使用域名获取公网地址去访问内网的服务器。



1. 将电脑的IP地址设置为：192.168.1.3，掩码为255.255.255.0。连接在ACG1040的ge0接口。在浏览器中输入https:192.168.1.1登录设备，设备默认的用户名和密码为“admin”。



2. 配置ge1为外网接口并配置IP地址。



3. 配置LAN接口的IP地址



基本设置

名称: (58:6a:b1:c4:54:c4)

启用:

IP类型: **IPv4** | IPv6

地址模式: 静态地址 | DHCP | PPPOE

接口主地址:

从IPv4列表:

地址	操作

管理方式: HTTPS | HTTP | SSH | Telnet | Ping

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

4. 配置到外网的路由，也就是运营商给的外网网关。

网络配置 > 路由 > 静态路由

静态路由

目的地址:

子网掩码:

下一跳/出接口: 下一跳 | 出接口

下一跳:

权重: (1-255)

距离: (1-255)

地址探测:

5. 设置源NAT

网络配置 > NAT

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:

测试已经可以上网（在客户端上ping外网网关地址）

```
C:\Users\Administrator>ping 198.76.28.1
正在 Ping 198.76.28.1 具有 32 字节的数据:
来自 198.76.28.1 的回复: 字节=32 时间<1ms TTL=128
来自 198.76.28.1 的回复: 字节=32 时间<1ms TTL=128
来自 198.76.28.1 的回复: 字节=32 时间<1ms TTL=128
来自 198.76.28.1 的回复: 字节=32 时间<1ms TTL=128
```

6. 映射内部一台telnet服务器

网络配置 > NAT

目的NAT

名称: (1-31字符)

描述: (0-127 字符)

地址项目: 子网地址 | 范围地址 | 主机地址 |

已添加项目	类型	地址	操作
1	host	198.76.28.2	<input type="button" value="删除"/>

地址池

名称 (1-31 字符)

地址项目 - [+ 添加到列表](#)

地址池	地址开始	地址结束	操作
1	192.168.2.3	192.168.2.3	删除

目的NAT规则

源地址 [+ 新建](#)

目的地址 [+ 新建](#)

服务

接口

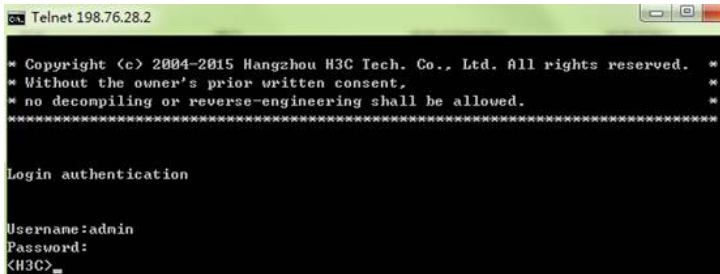
转换类型 地址映射 端口映射 不转换

转换后IP

日志

[提交](#) [取消](#)

测试结果外网可以使用198.76.28.2这个地址访问到telnet服务器。



7、（重点）使用内网电脑使用公网地址或者域名去访问内部的服务器。
配置源是内网网段的地址资源

新建地址对象

名称 (1-31字符)

描述 (0-127 字符)

地址项目 子网地址 范围地址 主机地址 [+ 添加到列表](#)

(例如: 192.168.1.1/24)

已添加项目	类型	地址	操作
1	network	192.168.2.0/24	删除

源NAT规则

源地址 [+ 新建](#)

目的地址 [+ 新建](#)

服务

接口

转换类型 出接口 地址池 不转换

日志

[提交](#) [取消](#)

配置目的NAT应用在内网接口。

目的NAT规则

源地址 [+ 新建](#)

目的地址 [+ 新建](#)

服务

接口

转换类型 地址映射 端口映射 不转换

转换后IP

日志

[提交](#) [取消](#)

实验测试结果：在内网也是可以登录。

```
Username:admin
Password:
<H3C>_
```

1. 在ACG配置目的NAT的时候，转换后的地址一定需要在地址池中创建。否则无法调用。
2. 在内网接口配置源NAT的时候一定要注意，源IP地址不能为“any”，如果为any那么外网内网访问外网的数据也会地址转换，导致无法访问网段
- 3.

4. 五 ACG NAT异常排查思路

- 1、 先使用内网电脑使用服务器内网的IP地址测试，服务器服务是否正常？
- 2、 在ACG网络诊断中ping一下服务器看服务器是否可达？
- 3、 排除运营商端口影响，可以将设备的http登录端口修改为要映射的端口，如果能正常访问那么就说明端口没有封掉，如果端口被封请联系运营商。
- 4、 收集设备的debugging信息。

在设备上首先输入：

```
H3C>enable
H3C# display log debug
删除debug
H3C# clear log debug
```



本次实验收集的debug信息.txt

有兴趣的同学可以对于debug信息研究一下，会发现：

- 1、 内网的数据上去匹配目的NAT

```
<2016-03-19 18:46:56> NAT: srclp:192.168.2.2,dstlp=198.76.28.1,outif=ge1,find source nat
rule:rule_id=1                \匹配到源NAT规则
<2016-03-19 18:46:56> NAT: NAT*: Setup the nat infors:
<2016-03-19 18:46:56> NAT: NAT*: 1 192.168.2.2 -> 198.76.28.1 >> 198.76.28.2 -> 198.76.28.1
                \将源地址进行转换
<2016-03-19 18:46:56> IPV4 198.76.28.2 > 198.76.28.1 ICMP Echo Request (send t
o ge1)
<2016-03-19 18:46:56> IPV4 198.76.28.1 > 192.168.2.2 ICMP Echo Reply (send to g
e2)
<2016-03-19 18:46:57> IPV4 198.76.28.2 > 198.76.28.1 ICMP Echo Request (send t
o ge1)
<2016-03-19 18:46:57> IPV4 198.76.28.1 > 192.168.2.2 ICMP Echo Reply (send to g
e2)
<2016-03-19 18:46:58> IPV4 198.76.28.2 > 198.76.28.1 ICMP Echo Request (send t
o ge1)
<2016-03-19 18:46:58> IPV4 198.76.28.1 > 192.168.2.2 ICMP Echo Reply (send to g
e2)
<2016-03-19 18:46:59> IPV4 198.76.28.2 > 198.76.28.1 ICMP Echo Request (send t
o ge1)
<2016-03-19 18:46:59> IPV4 198.76.28.1 > 192.168.2.2 ICMP Echo Reply (send to g
e2)
<2016-03-19 18:47:00> NAT: srclp:192.168.2.2,dstlp=10.165.6.49,outif=ge1,find source nat
rule:rule_id=1
```