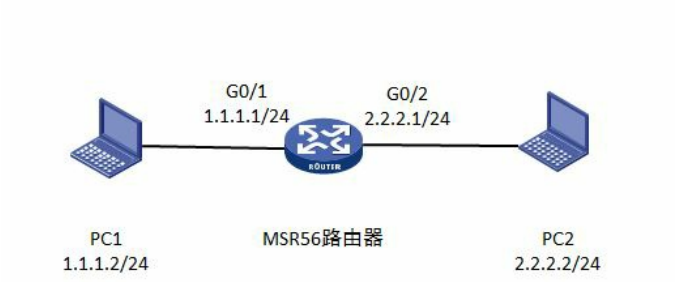
MSR56路由器通过acl控制接口间的访问

MDC ACL 李聪 2016-02-01 发表

一、功能需求

现在客户只有一台MSR56系列路由器的情况下需要对内网属于两个不同网段的客户端之间的访问进行控制。



二、 组网信息：

如图所示，路由器下面分别接着属于不同网段的客户端，pc1属于1.1.1.0/24网段，pc2属于2.2.2.0/24网段。现在要求pc1的电脑可以ping通pc2的电脑，但是pc2的电脑不可以ping通pc1；pc1的电脑可以使用tcp协议对pc2电脑进行访问，但是pc2 的电脑不可以使用tcp协议对pc1电脑的访问。

三、 组网需求：

1. acl控制列表的配置

1.1 配置acl3000的rule 0对icmp报文的控制。

rule 0 deny icmp source 2.2.2.0 0.0.0.255 destination 1.1.1.0 0.0.0.255 icmp-type echo //需要在G0/2接口上面引用，对pc2到pc1的icmp请求报文进行控制。

1.2 配置acl3000的rule 1对tcp报文的控制。

rule 1 deny tcp source 2.2.2.0 0.0.0.255 destination 1.1.1.0 0.0.0.255 ack 0 //需要在G0/2接口上面引用，对pc2到pc1的tcp报文进行控制。

2. acl3000在G0/2接口下的配置

2.1 将acl3000引用到G0/2接口

#

interface GigabitEthernet 0/2

ip address 2.2.2.1 255.255.255.0

packet-filter 3000 inbound //在G0/2接口下面调用acl3000，inbound方向。

四、 配置要点

1. 配置要点

1.1 acl的rule的配置需要根据acl引用在哪个接口，以及在接口引用acl的方向来确定。

1.2 如上的需求，如果引用在G0/1接口的inbound方向的话，acl3000应该配置如下：

#

acl advanced 3000

rule 0 deny icmp source 1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255 icmp-type echo-reply //针对pc1回应的icmp报文进行控制。

rule 1 deny tcp source 1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255 ack 1 //与以上配置作为比较，这次拦截的方向不同，拦截的tcp的ack报文方向也不一样。