MSR系列路由器使用TCP Established参数进行单向TCP访问控制功能的配置

丘子隽 2008-01-07 发表

MSR系列路由器
使用TCP Established参数进行单向TCP访问控制的配置

关键字：MSR; 防火墙; firewall; established; ACL; TCP

一、**组网需求**：
MSR两个接口分别连接2个FTP服务器，要求2.2.2.1可以FTP登录到1.1.1.10，而1.1.1.10不能FTP或Telnet到2.2.2.1。
设备清单：MSR系列路由器1台
二、组网图：

三、配置步骤：

MSR配置

```
#
 //使能防火墙
 firewall enable
#
//配置ACL 3000，即使用tcp established匹配TCP 3次握手中第2次握手报文
acl number 3000
 rule 0 deny tcp established
#
//连接2.2.2.1的接口，防火墙使用入方向ACL 3000，即过滤掉2.2.2.1发送的第二次握手报文，即1.1.1.10发起的TCP连接请求无法获得响应
interface GigabitEthernet0/0
 port link-mode route
 firewall packet-filter 3000 inbound
 ip address 2.2.2.2 255.255.255.0
#
//连接1.1.1.10的接口
interface GigabitEthernet0/1
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
#
```

四、**配置关键点**：
1) 使能防火墙；
2) ACL过滤掉TCP Established；
3) 在接口上注意防火墙使用的方向，不同的方向会有不同的效果，因为过滤的是3次握手中的第2次握手。