SR6600路由器ASPF防火墙功能的配置

管祥杰 2008-12-11 发表

SR6600路由器ASPF防火墙功能的配置

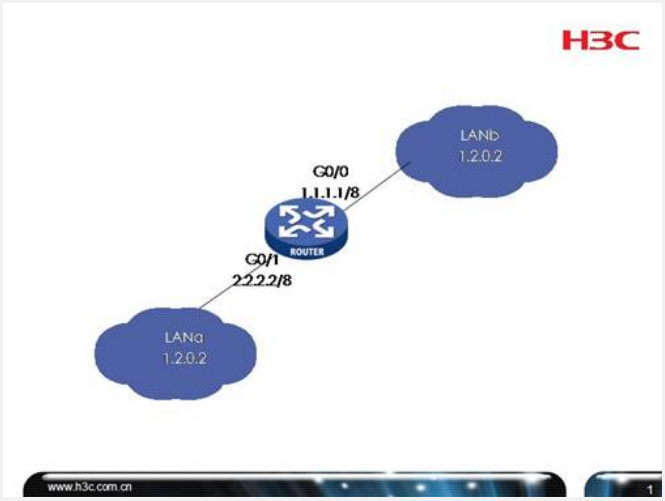
关键字：SR66;ASPF;防火墙

一、组网需求：

SR66作为LANa和LANb的网关，要求除了LANa访问LANb中FTP服务器的流量，禁止任何LANb到LANa的流量

设备清单：SR6600路由器1台，PC两台

二、组网图：



三、配置步骤：

SR66配置

```
#
 //全局打开防火墙，防火墙默认行为为允许
 firewall enable
#
//建立ASPF策略1
aspf-policy 1
 //使能检测FTP协议，FTP会话超时为300秒
 detect ftp aging-time 300
#
//定义ACL3000拒绝所有流量
acl number 3000
 rule 0 deny ip
#
//连接LANb接口
interface GigabitEthernet0/0
 port link-mode route
 //使能入方向包过滤防火墙，匹配ACL3000，即拒绝任何入方向流量
 firewall packet-filter 3000 inbound
 //使能出方向ASPF策略1
 firewall aspf 1 outbound
 ip address 1.1.1.1 255.0.0.0
#
//连接LANa的接口
interface GigabitEthernet0/1
 port link-mode route
 ip address 2.2.2.2 255.0.0.0
#
```

四、配置关键点：

1) 包过滤防火墙在此配置中要定义为inbound，如果定义为outbound则LANa和LANb任何连通性失败，路由器无法动态检测FTP使用的TCP端口

> 2) 在此组网中ASPF防火墙要配置为outbound方向