

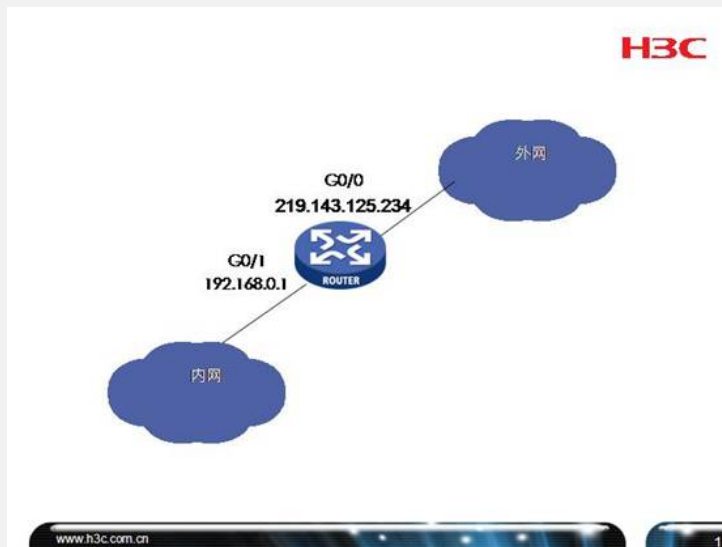
SR6600路由器包过滤控制访问列表的功能配置

关键词: SR66;ASPF;ACL

一、组网需求:

对内网地址192.168.1.22/25访问外网做限制,使其无法访问所有WEB界面;
但可以使用其它应用

二、组网图:



三、配置步骤:

RTA关键配置脚本

```
#
//使能防火墙功能
firewall enable
#
//配置防火墙缺省过滤方式为允许包通过
firewall default permit
#
dhcp server ip-pool 1
network 192.168.1.0 mask 255.255.255.0
gateway-list 192.168.1.1
dns-list 202.106.0.20 202.106.46.151
#
acl number 2000
rule 0 permit source 192.168.1.0 0.0.0.255
//定义用于包过滤的访问控制的ACL
acl number 3005
description deny_souce_ip_www
rule 0 deny tcp source 192.168.1.22 0 destination-port eq www
rule 5 permit tcp source 192.168.1.22 0
#
interface GigabitEthernet0/0
link-protocol ppp
ip address 219.143.125.234 255.255.255.252
nat outbound 2000
#
//对于inbound流量进行过滤
interface GigabitEthernet0/1
port link-mode route
ip address 192.168.1.1 255.255.255.0
firewall packet-filter 3005 inbound
#
ip route-static 0.0.0.0 0.0.0.0 Serial0/1
#
```

四、配置关键点:

1) 系统缺省情况下为禁止防火墙firewall disable, 需要使用命令“firewall enable”来使能防火墙功能。