H3C S9500交换机Firewall之ASPF策略组网应用的配置

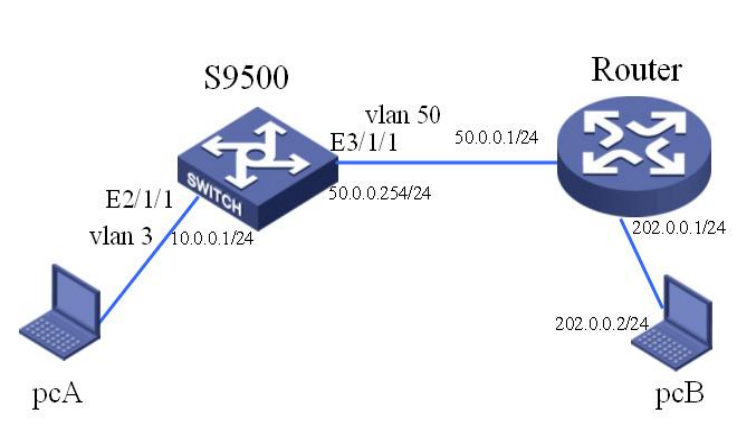
孟维佳 2006-11-06 发表

H3C S9500交换机Firewall之ASPF策略组网应用的配置

一、组网需求:

如下图所示，某公司通过SecBlade连接到Internet。内部某一主机地址为10.0.0.2，不允许外部任何外部的报文通过SecBlade访问内部主机，但如果是内部主机发起的ftp连接访问外部服务器资源，则其返回报文允许通过，假定外部开启ftp server的pcB的IP地址为202.0.0.2/24。本例可以应用在本地用户需要访问远程网络服务的情况下。

二、组网图



三、配置步骤

软件版本：H3C S9500交换机全系列软件版本

硬件版本：H3C S9500交换机LSM1FW8DB1防火墙业务板

1）添加内网VLAN 10，外网VLAN 50和SecBlade互连VLAN 30

[S9500] vlan 10

[S9500 - vlan10]port E2/1/1

[S9500] vlan 50

[S9500 - vlan50] port E3/1/1

[S9500] vlan 30

2）配置内网VLAN和互连VLAN配置接口地址

[S9500] interface vlan-interface 10

[S9500-Vlan-interface10] ip address 10.0.0.1 24

[S9500] interface vlan-interface 30

[S9500-Vlan-interface30] ip address 30.0.0.1 24

3）配置路由，外网报文下一跳为SecBlade防火墙

[S9500] ip route-static 0.0.0.0 0 30.0.0.254

4）配置SecBlade module，设置VLAN50为security-vlan，互连VLAN为VLAN30

[S9500]secblade module test

[S9500-secblade-test] secblade-interface vlan-interface 30

[S9500-secblade-test] security-vlan 50

[S9500-secblade-test] map to slot 2

5）进入SecBlade视图，配置互连子接口VLAN 30和外网子接口 VLAN 50（缺省用户名和密码为SecBlade，区分大小写）

<S9500> secblade slot 2

user：SecBlade

password：SecBlade

<SecBlade_FW> system

[SecBlade_FW] interface GigabitEthernet 0/0.50

[SecBlade_FW -GigabitEthernet0/0.50] vlan-type dot1q vid 50

[SecBlade_FW -GigabitEthernet0/0.50] ip address 50.0.0.254 24

[SecBlade_FW] interface g0/0.30

[SecBlade_FW -GigabitEthernet0/0.30] vlan-type dot1q vid 30

[SecBlade_FW -GigabitEthernet0/0.30] ip address 30.0.0.254 24

6）把互连子接口加入trust区域，外网子接口加入untrunst区域

[SecBlade_FW] firewall zone trust

[SecBlade_FW -zone-trust] add interface GigabitEthernet 0/0.30

[SecBlade_FW] firewall zone untrust
[SecBlade_FW -zone-untrust] add interface GigabitEthernet 0/0.50
7）配置路由，外网报文下一跳为路由器，内网报文下一跳为S9500
[SecBlade_FW] ip route-static 0.0.0.0 0 50.0.0.1
[SecBlade_FW] ip route-static 10.0.0.0 24 30.0.0.1
8）SecBlade视图下配置ACL和ASPF策略，检测FTP报文
[SecBlade_FW]firewall packet-filter enable
[SecBlade_FW-acl-adv-3111]acl number 3111
[SecBlade_FW-acl-adv-3111]rule deny ip
[SecBlade_FW]aspf-policy 1
[SecBlade_FW -aspf-policy-1]detect ftp aging-time 3000
9）SecBlade视图下把ASPF策略应用到外网子接口
[SecBlade_FW]interface GigabitEthernet 0/0.50
[SecBlade_FW -GigabitEthernet0/0.50]firewall aspf 1 outbound
[SecBlade_FW -GigabitEthernet0/0.50]firewall packet-filter 3111 inbound
四、配置关键点:
1）Secblade的用户名一定要注意分清大小写；
2）Firewall在缺省默认情况下对不符合规则的报文是不转发的，需要执行命令firewall packet-filter default permit使其默认转发；