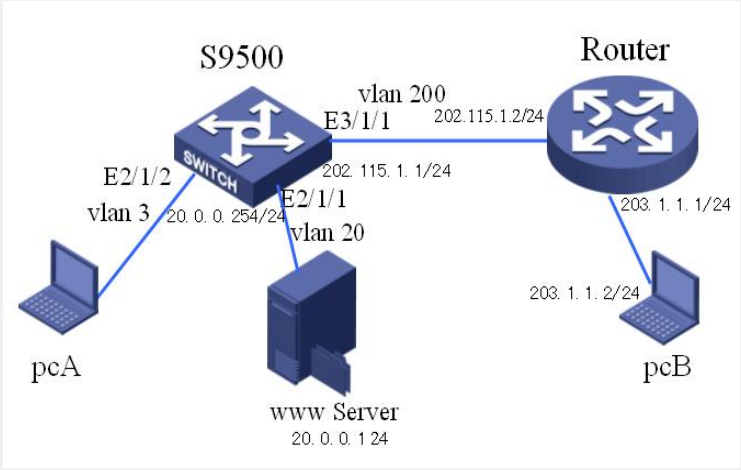
H3C S9500交换机Firewall之包过滤防火墙组网应用的配置

孟维佳 2006-11-06 发表

H3C S9500交换机Firewall之包过滤防火墙
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。公司内部对外提供WWW和FTP服务。其中，内部WWW服务器地址为20.0.0.1，只允许外部特定pcB可以访问内部服务器，但是不能访问内部网络的其他资源，假定外部特定用户pcB的IP地址为203.1.1.2/24，内部用户pcA的地址为3.1.1.2/24 。

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 20和VLAN 3，外网VLAN 200，Secblade互连VLAN 50
[S9500] vlan 20
[S9500 - vlan20]port E2/1/1
[S9500] vlan 3
[S9500 - vlan3]port E2/1/2
[S9500] vlan 200
[S9500 - vlan200] port E3/1/1
[S9500] vlan 50
2）配置内网VLAN接口IP地址
[S9500] interface vlan-interface 20
[S9500-Vlan-interface20] ip address20.0.0.254 24
[S9500] interface vlan-interface 3
[S9500-Vlan-interface3] ip address 3.1.1.1 24
[S9500] interface vlan-interface 50
[S9500-Vlan-interface50] ip address50.1.1.1 24
3）配置路由，发往外网的报文下一跳为SecBlade防火墙
[S9500] ip route-static 0.0.0.0 0 50.1.1.2
4）配置SecBlade module，设置VLAN200为security-vlan
[S9500]secblade module test
[S9500-secblade-test] secblade-interface vlan-interface 50
[S9500-secblade-test] security-vlan 200
[S9500-secblade-test] map to slot 2
5）进入SecBlade视图
<S9500> secblade slot 2 （缺省用户名和密码为SecBlade，区分大小写）
user：SecBlade
password：SecBlade
6）配置子接口，Secblade互连子接口VLAN 50，外网子接口 VLAN 200。把互连子接口加入trust区域，外网子接口加入untrunst区域
[SecBlade_FW] interface GigabitEthernet 0/0.50
[SecBlade_FW -GigabitEthernet0/0.50] vlan-type dot1q vid 50

[SecBlade_FW -GigabitEthernet0/0.50] ip address 50.1.1.2 24
[SecBlade_FW] interface g0/0.200
[SecBlade_FW -GigabitEthernet0/0.200] vlan-type dot1q vid 200
[SecBlade_FW -GigabitEthernet0/0.200] ip address 202.115.1.1 24
[SecBlade_FW] firewall zone trust
[SecBlade_FW -zone-trust] add interface GigabitEthernet 0/0.50
[SecBlade_FW] firewall zone untrust
[SecBlade_FW -zone-untrust] add interface GigabitEthernet 0/0.200
7）配置路由，外网下一跳为路由器，内网下一跳为S9500
[SecBlade_FW] ip route-static 0.0.0.0 0 202.115.1.2
[SecBlade_FW] ip route-static 20.0.0.0 24 50.0.0.1
[SecBlade_FW] ip route-static 15.0.0..0 24 50.0.0.1
8）SecBlade视图下配置ACL规则，指定特定用户访问内网用户
[SecBlade_FW] firewall packet-filter enable
[SecBlade_FW] acl number 3002
[SecBlade_FW-acl-adv-3002] rule permit tcp source 203.1.1.1 0 destination 20.0.0.1 0 destination-port eq 80
[SecBlade_FW-acl-adv-3002] rule permit tcp source 203.1.1.1 0 destination 20.0.0.2 0 destination-port eq 25
[SecBlade_FW-acl-adv-3002] rule deny ip
[SecBlade_FW-GigabitEthernet0/0.200] firewall packet-filter 3002 inbound

四、配置关键点：

1）SecBlade的用户名和密码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；