H3C S9500交换机Firewall之NAT组网的配置

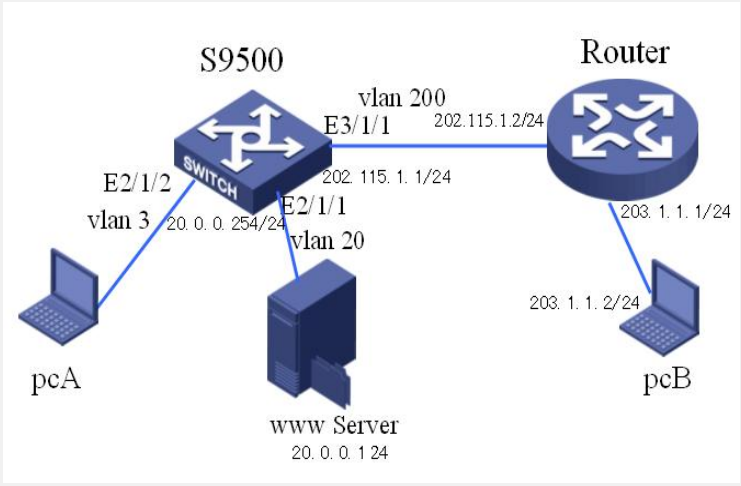
孟维佳 2006-11-18 发表

H3C S9500交换机Firewall之NAT组网的配置

一、组网需求:

外网用户通过访问防火墙上映射的公网地址来访问内部网络服务器，如下图所示，某公司通过Firewall的地址转换功能连接到Internet。公司内部对外提供www服务。其中，内部www服务器地址为192.168.2.1/24，并且希望可以对外提供统一的服务器的IP地址。内部192.168.3.0/24网段可以访问Internet，其它网段的PC机则不能访问Internet。外部的PC可以访问内部的服务器。公司具有202.115.1.1至 202.115.1.10十个合法的IP地址。选用202.115.1.1作为公司对外的IP地址。

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 - vlan2]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接口地址

[S9500] interface vlan-interface 20

[S9500-Vlan-interface2] ip address192.168.2.1 24

[S9500] interface vlan-interface 3

[S9500-Vlan-interface3] ip address 192.168.3.1 24

[S9500] interface vlan-interface 50

[S9500-Vlan-interface50] ip address50.0.0.1 24

3）配置默认路由，发往外网的报文下一跳指定为SecBlade防火墙

[S9500] ip route-static 0.0.0.0 0 50.0.0.2

4）配置SecBlade module，设置VLAN200为security-vla

[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（缺省用户名和密码为SecBlade，区分大小写）

<S9500> secblade slot 2

user：SecBlade

password：SecBlade

6）配置SecBlade互连子接口VLAN 50和外网子接口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 50.0.0.2 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，外网路由下一跳为路由器，内网路由下一跳为S9500
[SecBlade_FW] ip route-static 0.0.0.0 0 202.115.1.2
[SecBlade_FW] ip route-static 192.168.2.0 24 50.0.0.1
[SecBlade_FW] ip route-static 192.168.3.0 24 50.0.0.1
8）SecBlade视图下配置NAT地址池
[SecBlade_FW] nat address-group 1 202.115.1.2 202.115.1.10
9）SecBlade视图下配置ACL规则，指定可以通过NAT访问的内网用户，在接口绑定NAT
[SecBlade_FW] acl number 2001
[SecBlade_FW -acl-basic-2001] rule permit source 192.168.2.0 0.0.0.255
[SecBlade_FW -acl-basic-2001] rule permit source 192.168.3.0 0.0.0.255
[SecBlade_FW -acl-basic-2001] rule deny source any
[SecBlade_FW] interface GigabitEthernet 0/0.200
[SecBlade_FW -GigabitEthernet0/0.200] nat outbound 2001 address-group 1
10）设置内部服务器，给外网用户提供服务
[SecBlade_FW -GigabitEthernet0/0.200] nat server protocol tcp global 202.115.1.1 inside 20.0.0.1 www

四、配置关键点：

1） 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；
2） 进入SecBlade验证时注意字母大小写；
3） Pc上需要设置网关或默认路由；