H3C S9500交换机Firewall之地址绑定功能配置

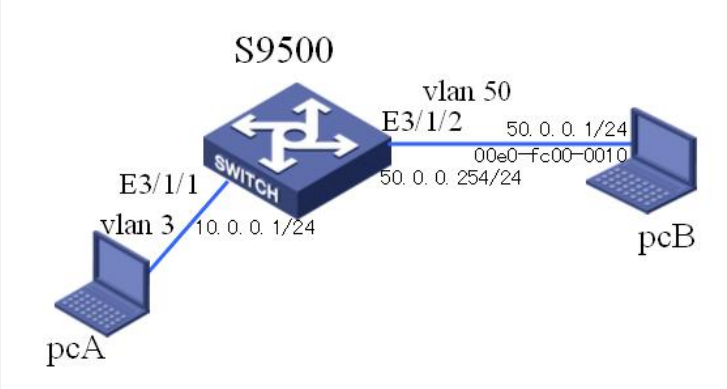
孟维佳 2006-11-15 发表

H3C S9500交换机Firewall之地址绑定功能配置

一、组网需求:

对客户机进行mac绑定处理，即客户机的ip地址只有发自绑定得mac地址后才会被防火墙处理，此功能对于ip防盗。服务器和客户机分别位于防火墙Trust区域和Untrust区域中，客户机的IP地址为50.0.0.1，对应的MAC地址为00e0-fc00-0100，在SecBlade上配置地址绑定关系，保证只有符合上述关系对的报文可以通过防火墙。

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，SecBlade互连VLAN 30

[S9500] vlan 10

[S9500 - vlan10]port E3/1/1

[S9500] vlan 50

[S9500 - vlan50] port E3/1/2

[S9500] vlan 30

2）为内网VLAN，服务器所在VLAN以及SecBlade互连VLAN配置地址

[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，设置外网VLAN为安全VLAN，进入SecBlade视图

[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

<S9500> secblade slot 2 （缺省用户名和密码为SecBlade，区分大小写）

user：SecBlade

password：SecBlade

<SecBlade_FW> system

5）进入SecBlade视图，配置子接口，并且把子接口加入相应的区域

[SecBlade_FW] interface GigabitEthernet 0/0.50

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

[SecBlade_FW -GigabitEthernet0/0.50] ip address 50.0.0.254 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

[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

6）配置路由，内网报文下一跳为S9500

[SecBlade_FW] ip route-static 10.0.0.0 24 30.0.0.1

7）SecBlade视图下配置地址绑定，配置客户机IP地址和MAC地址到地址绑定关系中
[SecBlade_FW] firewall mac-binding 50.0.0.1 00e0-fc00-0100
[SecBlade_FW] firewall mac-binding enable

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；