H3C S9500交换机Firewall之透明防火墙的配置

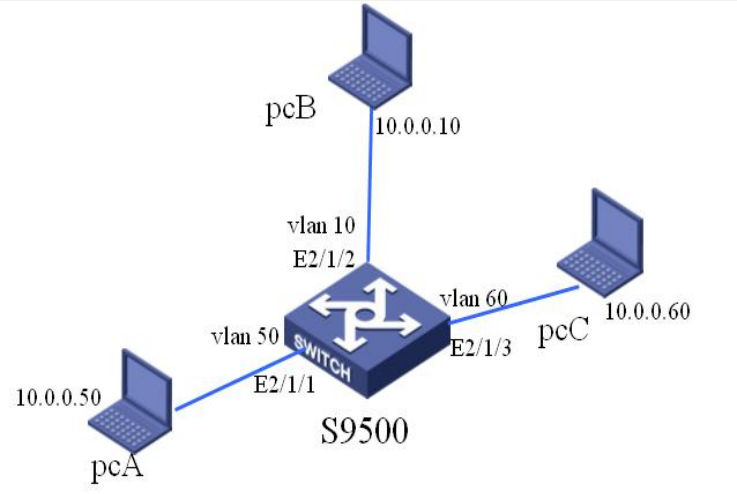
孟维佳 2006-11-18 发表

H3C S9500交换机Firewall之透明防火墙的配置

一、组网需求:

防火墙工作在透明模式下，并且使用基于MAC地址的访问控制列表允许Trust Zone中的主机访问DMZ Zone和Untrust Zone中的资源，并且使用黑名单阻止Untrust Zone中的主机PC_B发送的所有报文。S9500作为二层交换机，g3/1/1属于vlan30，g3/2/1属于vlan50，g3/3/1属于vlan60。其中主机pcA的IP地址为10.0.0.50，划归入DMZ区域，pcB的MAC地址为00e0-fc00-0100，划归入trust区域，pcC划归入untrust区域。

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DMZ VLAN 60

[S9500] vlan 10

[S9500 - vlan10]port E2/1/1

[S9500] vlan 50

[S9500 - vlan50] port E2/1/2

[S9500] vlan 60

[S9500 - vlan60] port E2/1/3

2）配置SecBlade module，设置这三个VLAN为安全VLAN

[S9500]secblade module test

[S9500-secblade-test] security-vlan 10 50 60

[S9500-secblade-test] map to slot 2

3）进入SecBlade视图，配置子接口，并且把子接口加入相应的区域（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

4）SecBlade视图下配置防火墙工作模式为透明模式，把接口加入相应的区域

[SecBlade_FW] firewall mode transparent.

[SecBlade_FW] firewall unknown-mac flood

[SecBlade_FW] interface GigabitEthernet 0/0.10

[SecBlade_FW -GigabitEthernet0/0.10] vlan-type dot1q vid 10

[SecBlade_FW] interface g0/0.50

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

[SecBlade_FW] interface GigabitEthernet 0/0.60

[SecBlade_FW -GigabitEthernet0/0.60] vlan-type dot1q vid 60

[SecBlade_FW] firewall zone trust

[SecBlade_FW -zone-trust] add interface GigabitEthernet 0/0.10

[SecBlade_FW] firewall zone untrust

[SecBlade_FW -zone-untrust] add interface GigabitEthernet 0/0.50
[SecBlade_FW] firewall zone DMZ
[SecBlade_FW -zone- DMZ] add interface GigabitEthernet 0/0.60
5）SecBlade视图下配置黑名单以及ACL
[SecBlade_FW] acl number 4000
[SecBlade_FW-acl-ethernetframe-4000] rule permit source-mac 00e0-fc00-0100 0000-0000-0000
[SecBlade_FW] interface GigabitEthernet 0/0.50
[SecBlade_FW -GigabitEthernet0/0.50] firewal ethernet-frame-filter 4000 outbound
[SecBlade_FW] interface GigabitEthernet 0/0.60
[SecBlade_FW -GigabitEthernet0/0.60] firewal ethernet-frame-filter 4000 outbound
[SecBlade_FW] firewall blacklist item 10.0.0.50 timeout 60
[SecBlade_FW] firewall blacklist 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） 防火墙透明模式下将未知mac报文的处理方式设置为flood；