SecBlade 防火墙单板透明模式的配置（一）

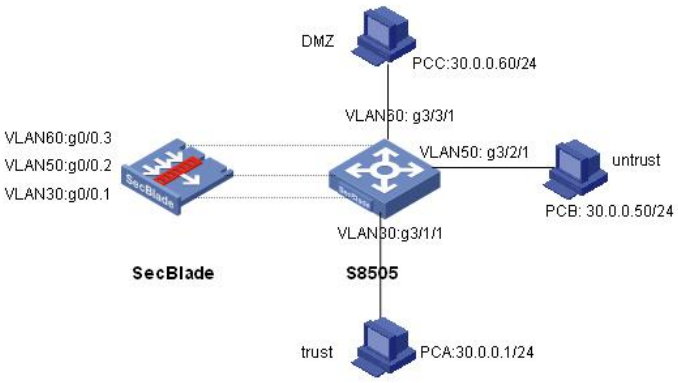
王思军　2006-09-17 发表

SecBlade 防火墙单板透明模式的配置（一）

一、 组网需求：

SecBlade防火墙单板工作在透明模式，S8500作为二层交换机。

二、 组网图：



SecBlade板工作在透明模式，S8505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。

软件版本如下：

S8505: VRP310-R1271

SecBlade：VRP3.4-ESS1209

三、 配置步骤：

本配置适用于S8500VRP3.1-R1271及以后版本，SecBlade VRP3.4-E1209及以后版本。

1、S8500配置

```
[S8505]dis cu
#
 config-version S8500-VRP310-r1271
#
 sysname S8505
#
 super password level 1 cipher O5(YaI!$LR+Q=^Q`MAF4<1!!
#
 local-server nas-ip 127.0.0.1 key huawei
#
 Xbar load-single
#
 router route-limit 128K
 router VRF-limit 256
#
 secblade aggregation slot 2    //配置内部端口聚合，增大带宽
#
radius scheme system
 server-type huawei
 primary authentication 127.0.0.1 1645
 primary accounting 127.0.0.1 1646
 user-name-format without-domain
#
domain system
 vlan-assignment-mode integer
 access-limit disable
 state active
 idle-cut disable
```

```
 self-service-url disable

 domain default enable system
#
vlan 1
#
vlan 30                  //创建vlan30、vlan50、vlan60
#
vlan 50
#
vlan 60
#
interface Aux0/0/1
#
interface M-Ethernet0/0/0
#
interface GigabitEthernet2/1/1
#
interface GigabitEthernet2/1/2
#
interface GigabitEthernet2/1/3
#
interface GigabitEthernet2/1/4
#
interface GigabitEthernet2/1/5
#
interface GigabitEthernet2/1/6
#
interface GigabitEthernet2/1/7
#
interface GigabitEthernet2/1/8
#
interface GigabitEthernet3/1/1    //PCA属于VLAN30
 port access vlan 30
#
interface GigabitEthernet3/1/2
#
interface GigabitEthernet3/1/3
#
interface GigabitEthernet3/1/4
#
interface GigabitEthernet3/2/1   //PCB属于VLAN50
 port access vlan 50
#
interface GigabitEthernet3/2/2
#
interface GigabitEthernet3/2/3
#
interface GigabitEthernet3/2/4
#
interface GigabitEthernet3/3/1   //PCC属于VLAN60
 port access vlan 60
#
interface GigabitEthernet3/3/2
#
interface GigabitEthernet3/3/3
#
interface GigabitEthernet3/3/4
#
interface NULL0
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
```

```
#
secblade module secblade
 security-vlan 30 50 60       //指定VLAN30、VLAN50、VLAN60为security-
vlan
 map to slot 2               //SecBlade板在二号槽位
#
return
[S8505]

[S8505]dis mac-address    //S8500的mac地址表项
MAC ADDR        VLAN ID    STATE           PORT INDEX            AGING TIME(s)
000f-e22c-9474    30       Learned         InnerPort slot 2       AGING
000f-e22c-9474    50       Learned         InnerPort slot 2       AGING
000f-e230-3754    60       Learned         InnerPort slot 2       AGING
000f-e230-3754    30       Learned         InnerPort slot 2       AGING
000f-e230-3748    50       Learned         InnerPort slot 2       AGING
000f-e230-3748    60       Learned         InnerPort slot 2       AGING
000f-e230-3748    30       Learned         GigabitEthernet3/1/1    AGING
000f-e230-3754    50       Learned         GigabitEthernet3/2/1    AGING
000f-e22c-9474    60       Learned         GigabitEthernet3/3/1    AGING

  ---  9 mac address(es) found  ---
[S8505]


2、SecBlade配置:
 <SecBlade_FW>dis cu
#
 sysname SecBlade_FW
#
 firewall packet-filter enable
 firewall packet-filter default permit        //防火墙设置包过滤缺省规则为permit

#
 firewall mode transparent               //将防火墙板设置为透明模式
 firewall unknown-mac flood          //将防火墙对未知mac报文的处理方式设置
为flood
#
 firewall statistic system enable
#
radius scheme system
#
domain system
#
interface Aux0
 async mode flow
#
interface Ethernet0/1
 promiscuous
#
interface Ethernet0/2
 promiscuous
#
interface Ethernet0/3
 promiscuous
#
interface GigabitEthernet0/0
 promiscuous
#
interface GigabitEthernet0/0.1
 vlan-type dot1q vid 30           //g0/0.1属于vlan30
#
interface GigabitEthernet0/0.2
 vlan-type dot1q vid 50           //g0/0.2属于vlan50
```

```
#
interface GigabitEthernet0/0.3
 vlan-type dot1q vid 60          //g0/0.3属于vlan60
#
interface NULL0
#
interface LoopBack0
 ip address 169.0.0.1 255.0.0.0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface GigabitEthernet0/0.1       //g0/0.1加入trust区域
 set priority 85
#
firewall zone untrust
 add interface GigabitEthernet0/0.2       //g0/0.2加入untrust区域
 set priority 5
#
firewall zone DMZ
 add interface GigabitEthernet0/0.3       //g0/0.3加入DMZ区域
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
user-interface con 0
user-interface aux 0
 authentication-mode password
user-interface vty 0 4
 authentication-mode scheme
#
return
<SecBlade_FW>

<SecBlade_FW>dis fir transparent-mode add  //透明防火墙的mac地址表
 The total of the address-items is 3
 Mac-address    Flag  Aging-time   Receive      Send  Interface-name
 000f-e230-3748  PD   00:03:59        38        10   GigabitEthernet0/0.1
 000f-e230-3754  PD   00:01:38        11         5   GigabitEthernet0/0.2
 000f-e22c-9474  PD   00:02:05        13         5   GigabitEthernet0/0.3
 Flag meaning:  P--PERMIT   N--DENY  D--DYNAMIC  S--STATIC
<SecBlade_FW>
```

四、 配置关键点：

1、防火墙透明模式下将未知mac报文的处理方式设置为flood。

```
firewall unknown-mac flood
```

2、注意将防火墙板内部子接口加入安全区域。