SecBlade 防火墙单板透明模式的配置（二）

王思军 2006-09-17 发表

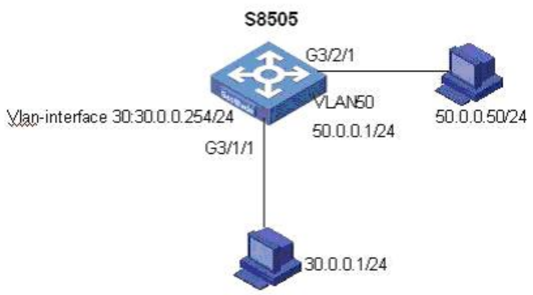
SecBlade 防火墙单板透明模式的配置（二）

一、 组网需求：

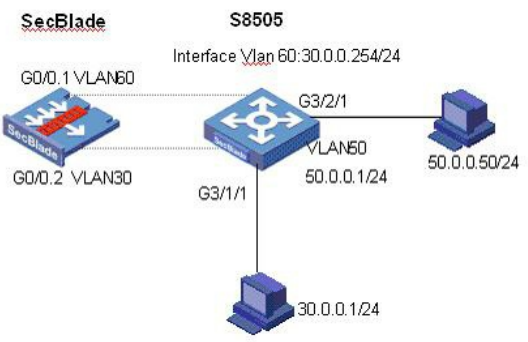
SecBlade防火墙单板工作在透明模式，内网和外网的网关终结在S8500上。

二、 组网图：

一般情况下，S8500工作在三层模式下，比如：S8500上配置两个interface vlan 30 /50分别作为内网和外网的vlan终结：



如果要在不改变现有网络情况下，增加SecBlade：



TRUST区域的通过S8500二层vlan30（security-vlan）转发到SecBlade，从SecBlade出来，打上vlan60的标签，终结在S8500的三层interface vlan60上，然后三层vlan50转发出去。

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
#
vlan 50
#
vlan 60
#
interface Vlan-interface50
 ip address 50.0.0.1 255.255.255.0
#
interface Vlan-interface60
 ip address 30.0.0.254 255.255.255.0
#
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              //内网PC属于VLAN30
 port access vlan 30
#
interface GigabitEthernet3/1/2
#
interface GigabitEthernet3/1/3
#
interface GigabitEthernet3/1/4
#
interface GigabitEthernet3/2/1
 port access vlan 50                   //外网PC属于VLAN50
#
interface GigabitEthernet3/2/2
#
interface GigabitEthernet3/2/3
```

```
#
interface GigabitEthernet3/2/4
#
interface GigabitEthernet3/3/1
#
interface GigabitEthernet3/3/2
#
interface GigabitEthernet3/3/3
#
interface GigabitEthernet3/3/4
#
interface NULL0
#
 ip route-static 0.0.0.0 0.0.0.0 50.0.0.50 preference 60
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
secblade module secblade
 security-vlan 30     //VLAN30指定为security-vlan，将该VLAN数据直接送
给SecBlade
 secblade-interface Vlan-interface60 //VLAN60为S8500与SecBlade内部三层接
口
 map to slot 2       //SecBlade板在2号槽位
#
return
<S8505>
<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 60       //g0/0.2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
 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]dis firewall transparent-mode address-table//透明防火墙的mac地址表
 The total of the address-items is 2
 Mac-address    Flag  Aging-time   Receive      Send  Interface-name
 000f-e21e-2204  PD   00:03:41        20        10   GigabitEthernet0/0.2
 000f-e230-3748  PD   00:03:39        33        10   GigabitEthernet0/0.1
 Flag meaning:  P--PERMIT   N--DENY  D--DYNAMIC  S--STATIC
```

四、 配置关键点:

1、 VLAN30三层不可终结在S8500上，否则VLAN30和VLAN50通过三层直接可达，数据将不通过SecBlade;通过将VLAN30设置为security-vlan将trust区域的数据送给SecBlade。

2、 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
```

3、 注意防火墙板内部子接口加入加入安全区域。