SecBlade 防火墙单板透明模式保护多VLAN的配置

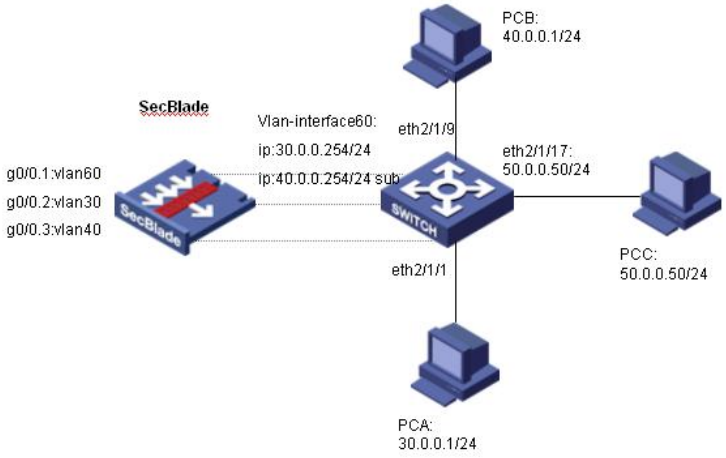
王思军　2006-11-08 发表

SecBlade 防火墙单板透明模式保护多VLAN的配置

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，内网有两个VLAN需要保护（VLAN30、VLAN40）。

二、 组网图：



软件版本如下：

S8505: VRP310-E1326

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

```
  [S9500B]dis cu
#
 config-version S8500-VRP310-E1326
#
 sysname S9500B
#
 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
#
 ip http directory
#
 mpls lsr-id 3.3.3.3
#
 vbas deviceid_type bridge_mac
#
 dldp interval 15
 dldp work-mode enhance
#
 secblade aggregation slot 4
#
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
#
 stp enable
#
vlan 1
#
vlan 30
#
vlan 40
#
vlan 50
#
vlan 60
#
interface Vlan-interface50              //外部接口
 ip address 50.0.0.1 255.255.255.0
#
interface Vlan-interface60              //与SecBlade内部接口
 ip address 30.0.0.254 255.255.255.0      //vlan30用户的网关
 ip address 40.0.0.254 255.255.255.0 sub   //vlan40用户的网关
#
interface Aux0/0/1
 flowcontrol normal
 async mode interactive
 link-protocol ppp
#
interface M-Ethernet0/0/0
#
interface Ethernet2/1/1
 port access vlan 30
#
interface Ethernet2/1/2

……
#
interface Ethernet2/1/8
#
interface Ethernet2/1/9
 port access vlan 40
#
interface Ethernet2/1/10
……

#
interface Ethernet2/1/17
 port access vlan 50
#
interface Ethernet2/1/18

……

#
user-interface con 0
user-interface aux 0
```

```
user-interface vty 0 4
 acl 2000 inbound
 user privilege level 3
 set authentication password simple 7-CZB#/YX]KQ=^Q`MAF4<1!!
#
secblade module secblade
 security-vlan 30 40                //vlan30、vlan40直接送给secblade
 secblade-interface Vlan-interface60   //vlan60为内部接口
 map to slot 4
#
return
[S9500B]
```

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
#
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        //与S8500的内部接口
 vlan-type dot1q vid 60
#
interface GigabitEthernet0/0.2      //VLAN30
 vlan-type dot1q vid 30
#
interface GigabitEthernet0/0.3      //VLAN40
 vlan-type dot1q vid 40
#
interface NULL0
#
interface LoopBack0
 ip address 169.0.0.1 255.0.0.0
#
firewall zone local
 set priority 100
#
firewall zone trust                //子接口加入安全域
 add interface GigabitEthernet0/0.2
```

```
 add interface GigabitEthernet0/0.3
 set priority 85
#
firewall zone untrust
 add interface GigabitEthernet0/0.1
 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]
```

四、 配置关键点：

1、 VLAN30/VLAN40三层不可终结在S8500上，否则VLAN30/VLAN40和VLAN50通过三层直接可达，数据将不通过SecBlade;通过将VLAN30/VLAN40设置为security-vlan将trust区域的数据送给SecBlade。

2、 S8500内部接口作为vlan30/vlan40的网关，由于secblade-interface Vlan-interface 只能有一个，因此，通过设置sub地址的方法。

```
interface Vlan-interface60                  //与SecBlade内部接口
ip address 30.0.0.254 255.255.255.0    //vlan30用户的网关
ip address 40.0.0.254 255.255.255.0 sub    //vlan40用户的网关
```

3、 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
```

4、 注意防火墙板内部子接口加入安全区域。