SecBlade防火墙单板NAT的配置

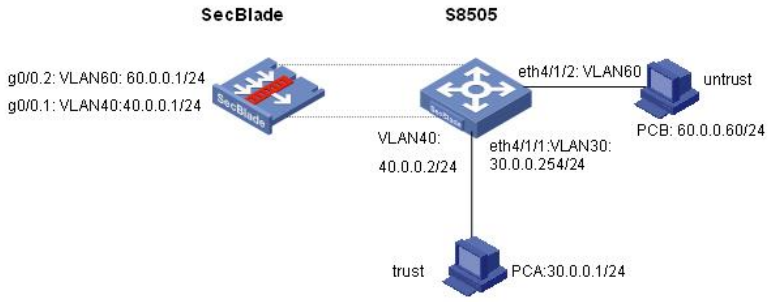
王思军　2006-09-17 发表

SecBlade 防火墙单板NAT的配置

一、 组网需求：

SecBlade防火墙单板作为NAT网关，内网的网关终结在S8500上。

二、 组网图：



要做NAT网关，SecBlade板只能工作在路由模式，S8505创建三层接口int Vlan-interface 40，作为与SecBlade的内部接口，内网PCA的网关在S8500上。防火墙板作nat，使trust区域的用户能访问公网，外网用户能通过公网地址访问DMZ区域的服务器。

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、vlan40、vlan60
#
vlan 40
#
vlan 60
#
interface Vlan-interface30          //内网网关
 ip address 30.0.0.254 255.255.255.0
#
interface Vlan-interface40
 ip address 40.0.0.2 255.255.255.0    //与SecBlade内部三层接口
#
interface Aux0/0/1
#
interface M-Ethernet0/0/0
#
interface Ethernet4/1/1         //eth4/1/1接内网
 port access vlan 30
#
interface Ethernet4/1/2         //eth4/1/2接外网
 port access vlan 60
#
interface Ethernet4/1/3
…… ……
#
interface NULL0
#
 ip route-static 0.0.0.0 0.0.0.0 40.0.0.1 preference 60  //通过路由，将数据送给Secblade
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
secblade module secblade
 security-vlan 60                //vlan60作为security-vlan，将外网数据送
到SecBlade
 secblade-interface Vlan-interface40   //vlan40为S8500与SecBlade的内部三层接
口
 map to slot 2                   //SecBlade板在2号槽位
#
return
[S8505]
[S8505]
[S8505]dis mac-address
MAC ADDR        VLAN ID    STATE           PORT INDEX            AGING TIME(s)
000f-e224-0ed7    60       Learned         InnerPort slot 2      AGING
000f-e224-0ed7    40       Learned         InnerPort slot 2      AGING
000f-e230-3748    30       Learned         Ethernet4/1/1         AGING
000f-e230-3754    60       Learned         Ethernet4/1/2         AGING

<S8505>dis arp
          Type: S-Static   D-Dynamic
IP Address      MAC Address     VLAN ID  Port Name             Aging Type
40.0.0.1        000f-e224-0ed7  40       InnerPort slot 2      19    D
30.0.0.1        000f-e230-3748  30       Ethernet4/1/1         18    D

---   2 entries found   ---
<S8505>
```

2、SecBlade配置：

```
[SecBlade_FW]dis cu
#
 sysname SecBlade_FW
#
 firewall packet-filter enable
 firewall packet-filter default permit      //包过滤缺省规则设置为permit
#
 firewall statistic system enable
#
radius scheme system
#
domain system
#
acl number 2000                        //用作nat outboundt的数据流
 rule 0 permit source 40.0.0.0 0.255.255.255
 rule 1 permit source 30.0.0.0 0.255.255.255
#
interface Aux0
 async mode flow
#
interface Ethernet0/1
#
interface Ethernet0/2
#
interface Ethernet0/3
#
interface GigabitEthernet0/0
#
interface GigabitEthernet0/0.1         //与S8500的内部接口
 ip address 40.0.0.1 255.255.255.0
 vlan-type dot1q vid 40
#
interface GigabitEthernet0/0.2         //外网接口
 ip address 60.0.0.1 255.255.255.0
 vlan-type dot1q vid 60
 nat outbound 2000                 //做nat转换
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust                  //内网接口加入trust域
 add interface GigabitEthernet0/0.1
 set priority 85
#
firewall zone untrust                //外网接口加入untrust域
 add interface GigabitEthernet0/0.2
 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
#
ip route-static 0.0.0.0 0.0.0.0 60.0.0.60 preference 60      //到公网的缺省路由
ip route-static 30.0.0.0 255.255.255.0 40.0.0.2 preference 60  //到内网的路由
 #
user-interface con 0
user-interface aux 0
 authentication-mode password
user-interface vty 0 4
 authentication-mode scheme
#
return
[SecBlade_FW]
 [SecBlade_FW]
[SecBlade_FW]
[SecBlade_FW]dis arp
          Type: S-Static   D-Dynamic
IP Address      MAC Address    Type Vpn-instance Name            Interface
40.0.0.2        000f-e21e-2204 D                                 GE0/0.1
60.0.0.60       000f-e230-3754 D                                 GE0/0.2

---   2 entries found   ---

[SecBlade_FW]dis nat session          //防火墙的NAT 会话表

There are currently 1 NAT session:

Protocol      GlobalAddr  Port      InsideAddr  Port       DestAddr  Port
      1       60.0.0.1 12288        30.0.0.1 43987       60.0.0.60 43987
              status:    11,        TTL: 00:01:00,       Left: 00:00:05
[SecBlade_FW]
```

四、 **配置关键点：**

1、SecBlade上要有到内网和外网的路由；S8500上要有到外网的路由，下一跳指向SecBlade。

2、注意将SecBlade子接口加入安全域。