SR66/SR66X系列路由器安全插卡与PBR组合多出口转发的典型配置

张玺 2013-07-15 发表

SR66/SR66X系列路由器安全插卡与PBR组合多出口转发的典型配置

关键字：SR66；SR66X；PBR；多出口

一、组网需求：

SR66/SR66X系列路由器支持防火墙插卡FWM-200、IPS插卡SPE-IPS-200以及ACG插卡SPE-ACG-200.

现在客户有一台SR6608路由器，希望在上面的某一入接口配置策略路由，使不同源地址的报文从不同的出接口转发，并且从这一入接口经过的双向报文被安全插卡处理。

本文以ACG插卡为例，IPS、FW插卡配置与ACG插卡类似。本文的配置可以通过策略路由实现源为100.0.0.1/32的报文从SR6608的G2/0/0接口转发，源为200.0.0.1/32的报文从SR6608的G2/0/1接口转发，且经过G5/0/0接口的双向报文均被ACG插卡处理。

设备及版本：SR6608路由器1台（版本为R2604P10）、SPE-ACG-200插卡1块（版本为ESS 6119P01）、MSR30-20路由器3台（版本为R2209P15）。

二、组网图：

三、配置步骤：

MSR1 配置
interface LoopBack0 ip address 50.0.0.1 255.255.255.255 # interface GigabitEthernet0/1 port link-mode route ip address 10.0.0.2 255.255.255.0 # ip route-static 0.0.0.0 0.0.0.0 10.0.0.1
MSR2 配置
interface LoopBack0 ip address 60.0.0.1 255.255.255.255 # interface GigabitEthernet0/1 port link-mode route ip address 11.0.0.2 255.255.255.0 # ip route-static 0.0.0.0 0.0.0.0 11.0.0.1
MSR3 配置

```
#
interface LoopBack0
 ip address 100.0.0.1 255.255.255.255
#
interface LoopBack1
 ip address 200.0.0.1 255.255.255.255
#
interface GigabitEthernet0/1
 ip address 12.0.0.2 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 12.0.0.1
#
```

SR6608配置

```
#
 acfp server enable     //使能ACFP服务器功能
#
 acsei server enable         //使能ACSEI服务器功能
#
acl number 3000
 rule 0 permit ip source 100.0.0.1 0
acl number 3001
 rule 0 permit ip source 200.0.0.1 0
#
vlan 1
#
vlan 100    //管理vlan
#
interface GigabitEthernet2/0/0
 port link-mode route
 ip address 10.0.0.1 255.255.255.0
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 11.0.0.1 255.255.255.0
#
interface GigabitEthernet5/0/0
 port link-mode route
 ip address 12.0.0.1 255.255.255.0
 ip policy-based-route h3c
#
interface Ten-GigabitEthernet3/0/0
 port link-mode route
 promiscuous     //内联口配置混杂模式
 ip policy-based-route h3c   //内联口配置和G5/0/0接口相同的PBR
#
interface Ten-GigabitEthernet3/0/0.1
 vlan-type dot1q vid 100
 ip address 100.100.100.1 255.255.255.0
#
policy-based-route h3c permit node 10
   if-match acl 3000
   apply ip-address next-hop 10.0.0.2
policy-based-route h3c permit node 20
   if-match acl 3001
   apply ip-address next-hop 11.0.0.2
#
ip route-static 100.0.0.1 255.255.255.255 12.0.0.2
 ip route-static 200.0.0.1 255.255.255.255 12.0.0.2
#
 snmp-agent
 snmp-agent local-engineid 800063A2030CDA41AFF186
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info version all
 snmp-agent group v3 v3group_no read-view iso write-view iso
 snmp-agent mib-view included iso iso
 snmp-agent usm-user v3 v3user_no v3group_no
#
```

ACG插卡配置

（1）　使用网线连接PC和ACG插卡的meth0/2口，PC配置地址192.168.1.2/24，ACG插卡meth0/2接口（要undo shutdown此接口）配置地址192.168.1.1/24，保证从PC能够ping通192.168.1.1。

（2）　打开浏览器，输入https://192.168.1.1进入ACG登录界面，输入用户名和密码后成功登录。

（3）　进入系统管理-网络管理-ACFP Client配置。配置OAA，确保连通性测试成功。

（4） 进入系统管理-网络管理-安全区域。创建内部安全区域，把需要引流的接口加入到安全域中。

（5） 进入系统管理-网络管理-段配置。在段配置中，把安全域关联为一个段，分别指定内部域和外部域为所创建的安全域。

（6） 进入系统管理-网络管理-ACFP联动策略。新建两条联动策略h3c和h4c，每条策略中“规则配置”里选择“所有报文”：

（7）　上述配置完成后，就可以正常引流了。在SR6608上查看，有ACFP策略生成：

```
[SR6608]dis acfp policy-info
ACFP policy total number: 2
ClientID:       1                 Policy-Index:  3
Rule-Num:       1                   ContextID:     2003
Exist-Time:     90       (s)      Life-Time:     2147483647(s)
Start-Time:     00:00:00           End-Time:      24:00:00
Admin-Status:   enable             Effect-Status: active
DstIfFailAction: delete            Priority:      4
In-Interface:   GigabitEthernet5/0/0
Out-Interface:
Dest-Interface:  Ten-GigabitEthernet3/0/0

ClientID:       1                 Policy-Index:  4
Rule-Num:       1                   ContextID:     2004
Exist-Time:     10       (s)      Life-Time:     2147483647(s)
Start-Time:     00:00:00           End-Time:      24:00:00
Admin-Status:   enable             Effect-Status: active
DstIfFailAction: delete            Priority:      4
In-Interface:
Out-Interface:  GigabitEthernet5/0/0
Dest-Interface:  Ten-GigabitEthernet3/0/0
```

四、功能测试：

完成以上配置后则引流成功。我们可以使用ACG的带宽管理功能，测试引流的成功性。

进入“带宽管理-策略管理。选择“新建策略应用”。

规则配置中使用“BLOCK”。确定后并“激活”，这样从100.0.0.1/32就无法访问50.0.0.1/32了。

```
<MSR3>ping -a 100.0.0.1 50.0.0.1
  PING 50.0.0.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
```

五、配置关键点：

1、 SR66/SR66X系列路由器不支持IPS/ACG混插组网，不支持二层组网。

2、 SR66/SR66X设备与安全插卡的内联口需配置为promiscuous 工作模式。

3、 内联子接口的VLAN ID要配置在1~2000以内。

4、 OAP插卡内联子接口仅用于OAA协议报文的协商。若想对引流的流量进行进一步操作，所做的配置都要在内联10GE主接口进行。如： PBR等功能都要配置在10GE主接口。

5、 该组网对于FW、IPS、ACG均有效。

6、 该方案要保证设备上的转发流的出入接口均不可有session相关应用存在（如：firewall，NAT等）。