SR66/SR66X系列路由器防火墙插卡与IPS/ACG插卡配合使用的典型配置

张玺 2013-07-15 发表

SR66/SR66X系列路由器防火墙插卡与IPS/ACG插卡配合使用的典型配置

关键字：SR66；SR66X；防火墙；IPS；ACG

一、组网需求：

SR66/SR66X系列路由器支持防火墙插卡SPE-FWM-200、IPS插卡SPE-IPS-200以及ACG插卡SPE-ACG-200.现在客户希望内网设备（使用MSR-1模拟）与外网设备（使用MSR-2模拟）之间的双向流量在经过出口路由器（使用SR6608模拟）时被防火墙插卡及IPS/ACG插卡处理。

本文以防火墙插卡与IPS插卡配合为例，ACG插卡配置与IPS插卡配置类似。

设备及版本：SR6608路由器1台（版本为R2604P10）、FWM-200插卡1块（版本为Release 3175）、SPE-IPS-200插卡1块（版本为ESS 2110P12）、MSR30-20路由器2台（版本为Release 2209P15）。

二、组网图：

三、配置步骤：

MSR-1 配置
interface GigabitEthernet0/1 port link-mode route ip address 20.0.0.2 255.255.255.0 # ip route-static 0.0.0.0 0.0.0.0 20.0.0.1
MSR-2 配置
interface LoopBack0 ip address 100.0.0.1 255.255.255.255 # 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
SR6608 配置

```
#
 acfp server enable        //使能acfp服务器
#
 acsei server enable         //使能acsei服务器
#
acl number 3000           //内网到外网的流量
 rule 0 permit ip source 20.0.0.0 0.0.0.255
acl number 3001           //外网到内网的流量
 rule 0 permit ip destination 10.0.0.0 0.0.0.255
#
vlan 1
#
vlan 100                //管理vlan
#
interface GigabitEthernet2/0/0
 port link-mode route
 ip address 20.0.0.1 255.255.255.0
 ip policy-based-route h3c1      //在SR6608的内网口上配置策略路由，下一跳是防火墙插卡的T0/0.1口
#
interface GigabitEthernet2/0/1
 port link-mode route
 ip address 10.0.0.1 255.255.255.0
 ip policy-based-route h3c2    //在SR6608的外网口上配置策略路由，下一跳是防火墙插卡的T0/0.2口
#
interface Ten-GigabitEthernet3/0/0.1
 vlan-type dot1q vid 1
 ip address 12.0.0.1 255.255.255.0
#
interface Ten-GigabitEthernet3/0/0.2
 vlan-type dot1q vid 2
 ip address 13.0.0.1 255.255.255.0
#
interface Ten-GigabitEthernet4/0/0        //与IPS插卡的内连口
 port link-mode route
 promiscuous              //配置为混杂模式
 ip policy-based-route h3c1       //和G2/0/0口配置相同的策略路由
#
interface Ten-GigabitEthernet4/0/0.1
 vlan-type dot1q vid 100       //管理vlan
 ip address 100.100.100.1 255.255.255.0
#
policy-based-route h3c1 permit node 10
 if-match acl 3000
 apply ip-address next-hop 12.0.0.2
#
policy-based-route h3c2 permit node 10
 if-match acl 3001
 apply ip-address next-hop 13.0.0.2
#
 ip route-static 100.0.0.1 255.255.255.255 10.0.0.2
#
 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
#
```

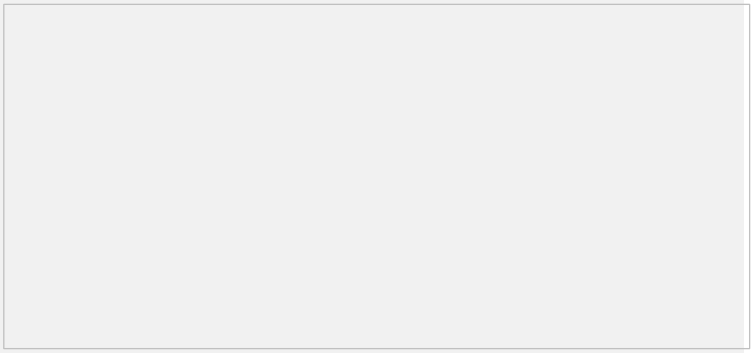
防火墙插卡配置

```
#
interface Ten-GigabitEthernet0/0.1
 vlan-type dot1q vid 1
 ip address 12.0.0.2 255.255.255.0
#
interface Ten-GigabitEthernet0/0.2
 vlan-type dot1q vid 2
 ip address 13.0.0.2 255.255.255.0
#
zone name Management id 0
 priority 100
 import interface GigabitEthernet0/0
zone name Trust id 2
 priority 85
 import interface Ten-GigabitEthernet0/0.1  //T0/0.1口加入Trust域
zone name Untrust id 4
 priority 5
 import interface Ten-GigabitEthernet0/0.2 //T0/0.2口加入Untrust域
#
 ip route-static 0.0.0.0 0.0.0.0 13.0.0.1    //去往外网的默认路由
 ip route-static 10.0.0.0 255.255.255.0 12.0.0.1  //去往内网的明细路由
#
```

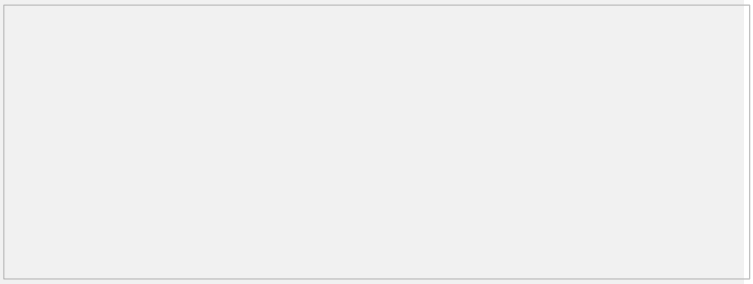
IPS插卡配置

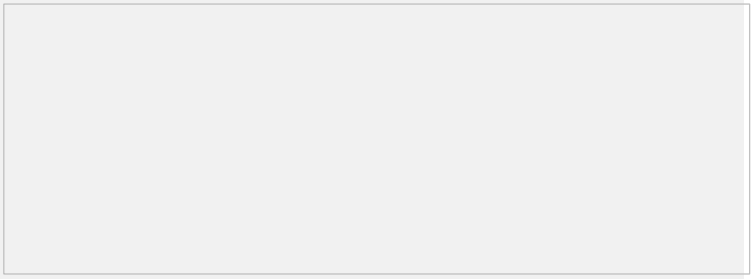
（1） 使用网线连接PC和IPS插卡的meth0/0口，PC配置地址192.168.1.2/24，IPS插卡meth0/0口（要undo shutdown此接口）配置地址192.168.1.1/24，保证从PC能够ping通192.168.1.1。
（2） 打开浏览器，输入https://192.168.1.1进入IPS登录界面，输入用户名和密码后成功登录。

（3） 进入系统管理-设备管理-OAA设置。配置OAA，确保连通性测试成功。

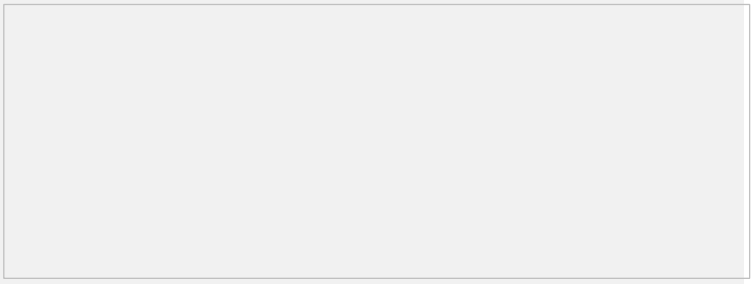


（4） 进入系统管理-网络管理-安全区域。创建内部安全区域，把需要引流的接口加入到安全域中。

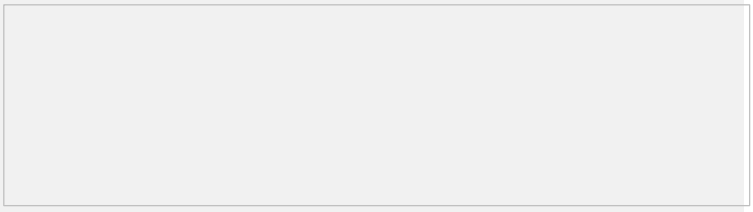




（5） 进入系统管理-网络管理-段配置。在段配置中，把安全域关联为一个段，分别指定内部域和外部域为所创建的安全域。



（6） 在相关应用下发相关策略，如：“IPS-段策略管理-创建策略应用”，“段”选择刚创建的段0，方向选双向。



（7） 最后点击激活按钮，把段策略下发到SR6608上，就可以正常引流了。

（8） 此时在SR6608上查看，有ACFP策略生成。

```
<SR6608>display acfp policy-info
ACFP policy total number: 2
ClientID:        1                  Policy-Index:  1
Rule-Num:        1                  ContextID:     2001
Exist-Time:      11820     (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:    GigabitEthernet2/0/0
Out-Interface:   GigabitEthernet2/0/1
Dest-Interface:  Ten-GigabitEthernet4/0/0

ClientID:        1                  Policy-Index:  2
Rule-Num:        1                  ContextID:     2002
Exist-Time:      11820     (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:    GigabitEthernet2/0/1
Out-Interface:   GigabitEthernet2/0/0
Dest-Interface:  Ten-GigabitEthernet4/0/0
```

四、功能测试：

完成以上配置后则引流成功。测试方法如下：

从MSR1上ping 100.0.0.1/32，可以ping通：

```
<MSR1>ping 100.0.0.1
  PING 100.0.0.1: 56  data bytes, press CTRL_C to break
    Reply from 100.0.0.1: bytes=56 Sequence=1 ttl=253 time=1 ms
    Reply from 100.0.0.1: bytes=56 Sequence=2 ttl=253 time=1 ms
    Reply from 100.0.0.1: bytes=56 Sequence=3 ttl=253 time=2 ms
    Reply from 100.0.0.1: bytes=56 Sequence=4 ttl=253 time=1 ms
    Reply from 100.0.0.1: bytes=56 Sequence=5 ttl=253 time=1 ms

  --- 100.0.0.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 1/1/2 ms
```

此时迅速在防火墙插卡上输入命令display session table，有session生成，这证明流量引上防火墙插卡成功：

```
<FW>dis session table
Initiator:
  Source IP/Port : 20.0.0.2/2048
  Dest IP/Port   : 100.0.0.1/2
  Pro            : ICMP(1)
  VPN-Instance/VLAN ID/VLL ID:
 Total find: 1
```

然后，使用IPS插卡的带宽管理功能。进入带宽管理-策略管理。选择“创建策略应用”。

规则配置中使用BLOCK。确定后并“激活”，这时从MSR-1 ping 100.0.0.1/32，发现无法ping通，内网无法访问外网。

```
<MSR1>ping 100.0.0.1
  PING 100.0.0.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
```

这证明流量引上OAA插卡成功。

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设备与安全板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、 SR6608的内网口G2/0/0上需同时配置PBR和ACFP，注意此时ACFP的优先级高于PBR）该步骤用于IPS插卡出问题时的流量逃生。