SR66/SR66X系列路由器与防火墙插卡配合开局的典型配置

张玺 2013-07-05 发表

SR66/SR66X系列路由器与防火墙插卡配合开局的典型配置

关键字：SR66；SR66X；防火墙

一、组网需求：

SR66/SR66X系列路由器支持防火墙插卡SPE-FWM-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）之间的流量在经过出口路由器（使用SR6608模拟）时被防火墙插卡处理。

设备及版本：SR6608路由器1台（版本为R3103P04）、SPE-FWM-200防火墙插卡1块（版本为R3175）、MSR30-20路由器2台（版本为R2209P15）。

二、组网图：

三、配置步骤：

MSR-1 配置

```
#
 sysname MSR1
#
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
#
```

MSR-2 配置

```
#
 sysname MSR2
#
interface LoopBack0
 ip address 100.0.0.1 255.255.255.255
#
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
#
```

SR6608 配置

```
#
 sysname 6608
#
acl number 3000   //匹配内网向外网发出的流量
 rule 0 permit ip source 10.0.0.0 0.0.0.255
acl number 3001   //匹配外网向内网发入的流量
 rule 0 permit ip destination 10.0.0.0 0.0.0.255
#
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
#
interface GigabitEthernet3/0/0
 port link-mode route
 ip address 11.0.0.1 255.255.255.0
 ip policy-based-route h3c2
#
interface GigabitEthernet3/0/1
 port link-mode route
 ip address 10.0.0.1 255.255.255.0
 ip policy-based-route h3c1
#
interface Ten-GigabitEthernet5/0/0    //内联口
 port link-mode route
#
interface Ten-GigabitEthernet5/0/0.1
 vlan-type dot1q vid 1
 ip address 12.0.0.1 255.255.255.0
#
interface Ten-GigabitEthernet5/0/0.2
 vlan-type dot1q vid 2
 ip address 13.0.0.1 255.255.255.0
#
 ip route-static 100.0.0.1 255.255.255.255 11.0.0.2
#
```

FW插卡配置

```
#
 sysname FW
#
interface Ten-GigabitEthernet0/0    //内联口
 port link-mode route
#
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 Trust id 2   //Trust域引入端口T0/0.1
 priority 85
 import interface Ten-GigabitEthernet0/0.1
zone name Untrust id 4    //Untrust域引入端口T0/0.2
 priority 5
 import interface Ten-GigabitEthernet0/0.2
#
 ip route-static 0.0.0.0 0.0.0.0 13.0.0.1
 ip route-static 10.0.0.0 255.255.255.0 12.0.0.1
#
```

四、功能测试：

配置完成后，从内网MSR-1 ping 外网MSR-2上的地址100.0.0.1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=252 time=2 ms
    Reply from 100.0.0.1: bytes=56 Sequence=2 ttl=252 time=2 ms
    Reply from 100.0.0.1: bytes=56 Sequence=3 ttl=252 time=1 ms
    Reply from 100.0.0.1: bytes=56 Sequence=4 ttl=252 time=2 ms
      Reply from 100.0.0.1: bytes=56 Sequence=5 ttl=252 time=1 ms
```

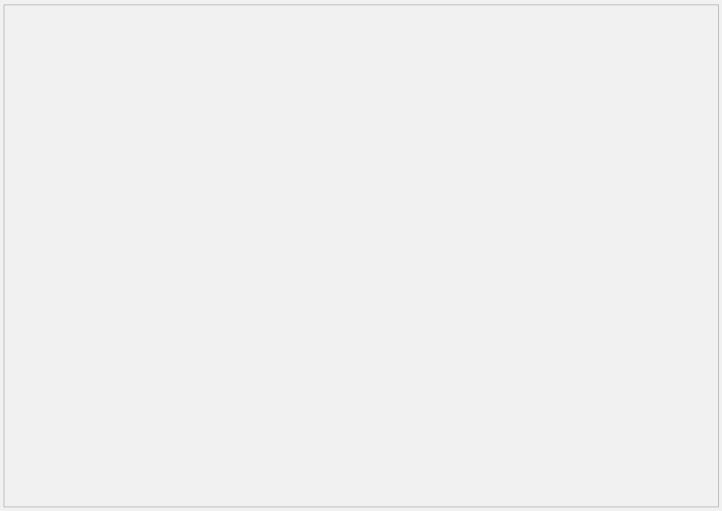
从FW上使用命令display session table可以看到相关的session：

```
[FW]dis session table
      Initiator:
      Source IP/Port : 10.0.0.2/2048
      Dest IP/Port   : 100.0.0.1/1
      Pro            : ICMP(1)
        VPN-Instance/VLAN ID/VLL ID:
```

从外网MSR-2 ping 内网MSR-1无法ping 通：

```
<MSR2>ping 10.0.0.2
  PING 10.0.0.2: 56  data bytes, press CTRL_C to break
    Request time out
        Request time out
```

需在防火墙插卡上做相关域间策略才能实现外网主动访问内网的功能。
通过WEB界面进入防火墙/安全策略/域间策略界面，进行如下配置：



配置完毕后，点击下方的“确定”按钮，域间策略创建成功。
此时从外网MSR-2带源100.0.0.1 ping 10.0.0.2能够ping 通：

```
<MSR2>ping -a 100.0.0.1 10.0.0.2
  PING 10.0.0.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.0.2: bytes=56 Sequence=1 ttl=252 time=2 ms
    Reply from 10.0.0.2: bytes=56 Sequence=2 ttl=252 time=1 ms
    Reply from 10.0.0.2: bytes=56 Sequence=3 ttl=252 time=2 ms
    Reply from 10.0.0.2: bytes=56 Sequence=4 ttl=252 time=1 ms
    Reply from 10.0.0.2: bytes=56 Sequence=5 ttl=252 time=1 ms
```

从外网MSR-2 ping 10.0.0.2无法ping通：

```
<MSR2>ping 10.0.0.2
  PING 10.0.0.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
```

五、配置关键点：
无