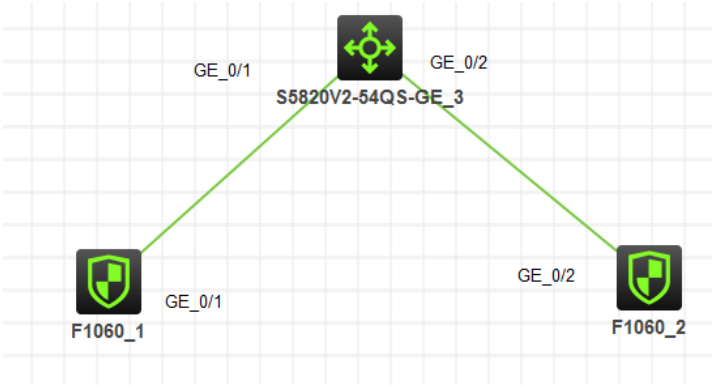
V7防火墙接口带vpn实例下的vrrp一直处于双主状态

李超 2018-02-01 发表

客户现场采用v7防火墙做vrrp，中间为二层交换机，发现vrrp一直处于双主状态，拓扑如下：



现场关键配置如下：

```
#
interface GigabitEthernet1/0/1
  port link-mode route
  combo enable copper
  ip binding vpn-instance IMS_OM
  ip address 10.181.161.2 255.255.255.0
  vrrp vrid 1 virtual-ip 10.181.161.1
  vrrp vrid 1 priority 105
#
security-zone name Trust
  import interface GigabitEthernet1/0/1
#
zone-pair security source Local destination Trust
  packet-filter 2000
  packet-filter name local_trunk
#
zone-pair security source Trust destination Local
  packet-filter 2000
  packet-filter name trust_local
#
acl advanced name local_trunk
  rule 107 permit ip vpn-instance IMS_OM
#
acl advanced name trust_local
   rule 100 permit ip
  rule 107 permit ip vpn-instance IMS_OM
```

查看两端vrrp状态，均属于master。

在设备上面debug vrrp packet，可以看到设备发了vrrp的通告报文。

```
<H3C>u*Feb  1 10:20:43:581 2018 H3C VRRP4/7/Packet: -COntext=1;
Sent Advertisement message from GigabitEthernet1/0/1
VRID: 1  Pri: 105  Adver timer: 100 centisecs
```

通过在中间交换机抓包，发现没有抓到vrrp的报文，怀疑被设备丢弃，在设备上debug域间策略情况，发现vrrp的通告报文被域间策略策略丢弃。

```
*Feb  1 10:20:43:582 2018 H3C FILTER/7/PACKET: -COntext=1; The packet isdenied. Src-ZOne=L
ocal, Dst-ZOne=Trust;If-In=InLoopBack0(1284), If-Out=GigabitEthernet1/0/1(2); Packet Info:Src-IP=1
0.181.161.2, Dst-IP=224.0.0.18, VPN-Instance=,Src-Port=0, Dst-Port=0, Protocol=VRRP(112), Appli
cation=invalid(0), ACL=none, Rule-ID=none.
```

vrrp的通告报文属于本地协议报文，从debug里面可以看到是没有vpn实例的，而设备上local到trust的域间策略中只放通的带vpn的策略，没有放通非vpn实例的策略，导致被域间策略丢弃。

在local到trust的域间策略中增加非vpn实例的策略。

```
acl advanced name local_trunk
    rule 107 permit ip vpn-instance IMS_OM
    rule 110 permit ip
```

此时vrrp状态正常。