M9000 SSLVPN拨号成功但访问IP资源不通问题

SSL VPN　**西海华**　2016-03-17 发表

问题现象：
M9000作为SSLVPN网关，客户端SSLVPN拨号成功后，客户端10.100.100.1 ping内网资源10.250.250.2（内网交换机接口IP），网络不通。

SSLVPN拨号成功后，PC10.100.100.1 ping内网资源10.250.250.2，看会话是建在slot7上，有发包没回包,debug显示被slot1 的aspf丢弃了。
*Feb 24 17:13:54:398 2016 M9010 ASPF/7/PACKET: -Slot=1.1; The first packet was dropped by ASPF for invalid status. Src-Zone=Trust, Dst-Zone=Trust;If-In=GigabitEthernet2/0/24(154), If-Out=SSLVPN-AC1(4695); Packet Info:Src-IP=10.250.250.2, Dst-IP=10.100.100.1, VPN-Instance=none,Src-Port=1, Dst-Port=0. Protocol=ICMP(1).

SSLVPN本身不下引流规则，目的地址是SSLVPN GW（111.75.206.107）的HTTPS报文上设备，出问题时上slot7，经过SSLVPN处理后内层走隧道 10.100.100.1 -> 10.250.250.2 ICMP，从slot7发送。
由于用户配置了NAT SERVER：nat server protocol tcp global 111.75.206.47 23 inside 10.250.250.2 23
下发如下引流规则：

Flow entry 136 information:
cookie: 0x0, priority: 5700, hard time: 0, idle time: 0, flags: check_overlap
|reset_counts|no_pkt_counts|no_byte_counts, byte count: --, packet count: --
Match information:
IP Range: IPv4 source address　　from 10.250.250.2 to 10.250.250.2
Instruction information:
Write actions:
　Group: 4026531849

导致反向报文上另外blade（当前应该上了slot1），进而被ASPF丢弃。

1、把目的地址到111.75.206.107 的报文通过mqc 引流到slot 1 上。
2、M9K IP接入必须配合NAT OUTBOUND一起使用，请在GigabitEthernet2/0/24下增加下 nat outbound,使得出去的报文反向也能回到这个卡 。

```
#
traffic classifier sslvpn operator and
if-match acl 3710
#
acl advanced 3710
description SSL_VPN_MQC
rule 10 permit ip destination 111.75.206.107 0
#
traffic behavior sslvpn
redirect interface Blade1/0/1
#
qos policy sslvpn
classifier sslvpn behavior sslvpn
#
interface GigabitEthernet2/0/20
qos apply policy sslvpn inbound enhancement
#
interface GigabitEthernet2/0/24
port link-mode route
combo enable copper
ip address 10.250.250.1 255.255.255.0
nat outbound 3088 address-group 77
#
nat address-group 77
```

address 10.250.250.7 10.250.250.11
#
acl advanced 3088
description SSLVPN-destination
rule 0 permit ip
#

sslvpn不下发引流规则（随机HASH到某个业务板），在配合NATSERVER使用时（NATSERVER会下发引流规则到另外的业务板）冲突导致的。只有SSLVPN拨号后访问目的地址为NATSERVER内部服务器地址时，才会出现该问题（比如10.250.250.2），该方案为规避措施。目前sslvpn不下发引流规则已提需求解决。