

## 知 S12500 OAA插卡内联口ACL不生效案例

OAA 产品特性 程飞 2015-10-30 发表

现网S125 IRF系统中，插入OAA板卡(IPS,FW)。报文二层到交换机,然后二层到IPS插卡处理后回到S12508，网关在S12508上。配置完成后，发现下联服务器与网关不通。为了防止环路，只允许访问网关地址的报文通过。

acl number 4000

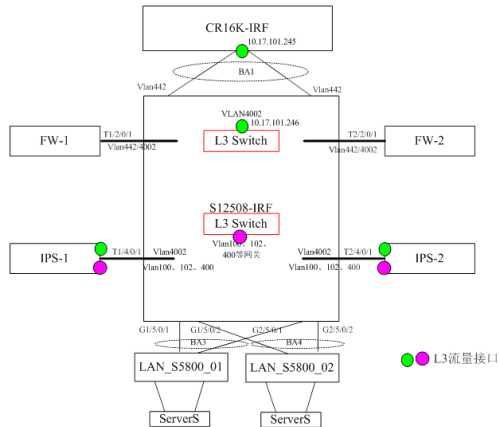
```
rule 0 permit type 0800 ffff dest-mac 000f-e22e-94b3 ffff-ffff-ffff
```

```
rule 1 permit type 88a7 ffff
```

```
rule 5 deny
```

```
interface Ten-GigabitEthernet3/0/1
```

```
packet-filter 4000 outbound
```



配置中默认有如下配置:

```
acl ipv6 disable
```

与现场配置[acl ipv6 disable](#)有关，该命令作用为将EC、EF类单板acl规则长度改为40字节，但是当acl规则长度为40字节时，该acl在出方向下发则不支持匹配ipv4的目的mac地址，现场的IPS插卡和FW插卡都是EC单板.packet filter和mqc都是下发在这些OAA插卡的内联口的，acl num 4000中rule 0为匹配目的mac，所以无法生效,进而匹配了rule5的deny规则,因此出现网关不通的问题。

将[acl ipv6 disable](#)改为[acl ipv6 enable](#)，然后重启整框。