# 防火墙ping自身地址不通

域间策略/安全域 ASPF 攻击防范 罗书鹏 2023-12-25 发表

## 组网及说明

不涉及

## 告警信息

不涉及

## 问题描述

防火墙RBM开局，发现在防火墙命令行ping自身地址不通。
接口配置很简单：

```
interface GigabitEthernet1/0/0
port link-mode route
combo enable copper
ip address 110.123.12.21 255.255.255.0
```

## 过程分析

可以通过debug查看报文处理情况
Debug ip info 显示被atk攻击防范丢了。
*Oct 24 16:24:24:891 2023 F5000M IPFW/7/IPFW_INFO: -COntext=1;
MBUF was intercepted! Phase Num is 4(local in beforedefrag), Service ID is 2(atk), Bitmap is 2000000000000000, return 1(0:continue, 1:dropped, 2:consumed, 3:enqueued, 4:relay)! Interface is InLoopBack0,
s=110.123.12.21, d= 110.123.12.21, protocol= 1, pktid = 11185
VsysID = 1.
看配置local应用了攻击防范，丢弃源目ip一样的报文，所以自己ping自己不通。

```
#
security-zone name Local
attack-defense apply policy abc
#
#
attack-defense policy abc
syn-flood detect non-specific
syn-flood action logging
 udp-flood detect non-specific
udp-flood action logging
 icmp-flood detect non-specific
icmp-flood action logging
 icmpv6-flood detect non-specific
icmpv6-flood action logging
 signature detect fragment action drop logging
signature detect impossible action drop logging
```

| | |
|---|---|
| Impossible | 攻击者通过向目标主机发送源IP地址和目的IP地址相同的报文，造成主机系统处理异常。 |

## 解决方法

将security-zone name Local视图下的attack-defense apply policy abc 删除即可