某局点过防火墙大包不通问题的经验案例

攻击防范 姜霁琛 2019-07-26 发表

组网及说明

B院区 核心——fw（1口）——（2口）msr——专线——（99.34）125　A院区，防火墙是二层透传，型号F1030，版本为D012分支的9313P07

问题描述

现场在b院区内部ping内部服务器大包均正常，但是只要经过防火墙，则ping大包不通，具体测试为ping到4000以上就不通了，4000以下的包可以正常ping通；从a院区125交换机经过专线ping出口msr路由器大包也正常，但经过防火墙后大包不通

过程分析

收集现场配置，接口超长帧放行默认开启，查看安全策略均为rule pass全放通，未做特殊限制，ping大包测试时在防火墙上收集会话信息，发现有会话，但是只有init发起方的包，没有respond响应方向的包。

```
Slot 1:
Initiator:
  Source      IP/port: 192.168.126.x/1
  Destination IP/port: 192.168.99.x/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Vlan-interface99
  Source security zone: Trust
Responder:
  Source      IP/port: 192.168.99.x/1
  Destination IP/port: 192.168.126.x/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: ICMP_REQUEST
Application: ICMP
Start time: 2019-07-26 09:14:18  TTL: 55s
Initiator->Responder:          8 packets      12000 bytes
Responder->Initiator:          0 packets          0 bytes

Total sessions found: 1
```

解决方法

继续检查防火墙的配置，发现该防火墙上开启了攻击防范功能，并且启用了icmp-flood攻击防范，在防火墙web上看到有很多相关的攻击日志，怀疑是流量被当做了泛洪攻击，而查看相关配置指导，icmp-flood攻击默认门限值为1000pps，后续现场将icmp-flood攻击门限值改大到10000后问题解决。

```
# attack-defense policy defense
  icmp-flood threshold 10000
```