

知 SecPath F5000-M(V7) 源nat 不通, 从公网口收到的回包被丢弃

NAT 王昕宇 2023-10-19 发表

组网及说明

目的端服务器-----公网----- fw-----内网---pc源

pc ping 服务器 不通

告警信息

debugging ip packet 发现回包被路由备用丢弃
prompt: FIB BLACKHOLE.

IPFW/7/IPFW_PACKET: -Context=1;

Discarding, interface = Route-Aggregation1.1

version = 4, headlen = 20, tos = 0, pktlen = 84, pktid = 2203, offset = 0, ttl = 251, protocol = 1

checksum = 9440, s = 1.1.1.1, d = 2.2.2.2, channelId = 0, vpn-InstanceIn = 1, vpn-InstanceOut = 0.

VsysID = 1

prompt: FIB BLACKHOLE.

Payload: ICMP type = 0, code = 0, checksum = 0x680b.

问题描述

源nat不通，源nat 不通，从公网口收到的回包被丢弃

过程分析

外网口配置了vpn实例， nat outbound后没有加vpn实例

```
interface Route-Aggregation1.1
```

```
ip binding vpn-instance test
```

```
ip address 3.3.3.3
```

```
nat outbound address-group 1
```

解决方法

```
interface Route-Aggregation1.1
```

```
nat outbound address-group 1 vpn-instance test
```

接口下修改如上配置后正常

出口有vpn实例，nat中也要配置vpn实例

否则 流量匹配不上会话就查路由命中黑洞（地址池中的地址暴露出去产生指向null的路由）

```
[H3C]session statistics enable
```

```
<H3C>display session table ipv4 source-ip 发起端ip destination-ip 发起端访问的目的地址 verbose
```

```
Responder:  
Source IP/port: [redacted] 9/11  
Destination IP/port: [redacted] 39/0  
DS-Lite tunnel peer: -  
VPN instance/VLAN ID/Inline ID: -/-/-  
Protocol: ICMP(1)  
Inbound interface: [redacted]  
Source security zone: C [redacted]  
State: ICMP_REQUEST
```

