某局点F1060过IPSec无法SSH登录设备本身问题

冗余组 IPSec VPN 孙轶宁 2021-06-30 发表

组网及说明

两台F1060做了IRF堆叠，冗余主备组网，作为出口设备跟其他设备对接IPSec。

问题描述

现场反馈通过ipsec隧道尝试ssh设备提示超时，但是在内网ssh设备或者在公网直接ssh公网口地址是没有问题的。

过程分析

1、首先debugging ssh server all发现没有任何输出，但是debugging ip packet能够看到端口22的ssh报文上送设备

2、查看display system internal aspf statistics zone-pair ipv4，当ssh超时的时候，First packets that failed status checking在不停增长

3、查看ssh会话，发现流量有跨框的现象。

Slot 1:

.....

Initiator->Responder: 1 packets 61 bytes

Responder->Initiator: 0 packets 0 bytes

Slot 2:

.....

Initiator->Responder: 0 packets 0 bytes

Responder->Initiator: 1 packets 61 bytes

4、检查冗余组跟irf状态，发现冗余组的primary节点在slot1，但是irf的master设备是slot2，导致上cpu的流量出现了跨框的情况，而客户没有配置ipsec redundancy enable同步ipsec会话信息，导致过ipsec隧道d流量跨框不通。

解决方法

开启ipsec redundancy enable后问题解决。