F5030(V7) L2TP OVER IPSEC拨号不成功问题

L2TP over IPSec VP 刘宏宇 2019-10-29 发表

问题描述

客户现网中使用F5030做出口设备， 原先loopback 1口为l2tp外网接入接口，可以正常拨号接入，现在使用loopback 2口作为l2tp over ipsec外网接入接口， l2tp over ipsec拨号提示ike协商失败。

解决方法

一、设备配置排查----查看关键基本配置没啥明显问题

对应inode客户端上ipsec参数配置--------跟设备配置也是对应的

二、测试终端取消ipsec，去勾选“启用IPSEC安全协议”，只测试L2T拨号正常，确实是ipsec问题，与inode报错“IKE协商失败”应该一致，重点排查ipsec相关内容，查看ipsec sa为空，ike sa如下

三、debug ike/ipsec分析：

Debug能看到两个ip之间的正常交互报文，ipsec第二阶段协商失败，提示INVALID_ID_INFORMATIO N

*Oct 10 12:09:49:500 2018 H3C IKE/7/EVENT: -COntext=1; vrf = 0, local = 59.x.x.245, remote = 27.x .x.192/27998

IPsec SA state changed from IKE_P2_STATE_INIT to IKE_P2_STATE_GETSP.

*Oct 10 12:09:49:500 2018 H3C IPSEC/7/EVENT: -COntext=1;

Could not find tunnel, ike profile name is 1.

*Oct 10 12:09:49:500 2018 H3C IPSEC/7/EVENT: -COntext=1;

Could not find tunnel, ike profile name is 1.

*Oct 10 12:09:49:500 2018 H3C IKE/7/EVENT: -COntext=1; Received message from ipsec, message type is 10.

*Oct 10 12:09:49:500 2018 H3C IKE/7/ERROR: -COntext=1; vrf = 0, local = 59.x.x.245, remote = 27. x.x.192/27998

Failed to get IPsec policy for phase 2 responder. Delete IPsec SA.

*Oct 10 12:09:49:500 2018 H3C IKE/7/ERROR: -COntext=1; vrf = 0, local = 59.x.x.245, remote = 27. x.x.192/27998

Failed to negotiate IPsec SA.

*Oct 10 12:09:49:500 2018 H3C IKE/7/EVENT: -COntext=1; Delete IPsec SA.

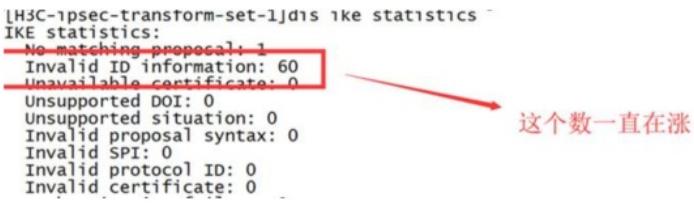
*Oct 10 12:09:49:501 2018 H3C IKE/7/PACKET: -COntext=1; vrf = 0, local = 59.x.x.245, remote = 27. x.x.192/27998

Encrypt the packet.

*Oct 10 12:09:49:501 2018 H3C IKE/7/PACKET: -COntext=1; vrf = 0, local = 59.x.x.245, remote = 27. x.x.192/27998

Construct notification packet: INVALID_ID_INFORMATION.

且查看ike报文情况



对于INVALID_ID_INFORMATION，之前整理有如下情况，但是目前案例都未命中

NVALID_ID_INFORMATION 身份无效

通常在IKE第二阶段协商时出现，常见的故障点有：

IPSec policy下配置的local-address与协商报文的IP地址不匹配

IPSec policy下配置的remote-address与协商报文的IP地址不匹配

接口下配置的IPSec policy名字错误

IKE SA协商的id-type类型不一致

对于协商ip地址都正确，但是设备为何会弹出身份标识ID错误信息，对比和正常案例发现应用接口为loopback接口，联系L3 确认loopback口无法正常处理ipsec报文，环回口没有进出接口的概念，自己配置模拟测试确实如此，跟客户现场环境是一样的debug报错信息。

【解决方法】

将ipsec policy从loopback环回口取消，在物理口上应用后ipsec sa建立正常