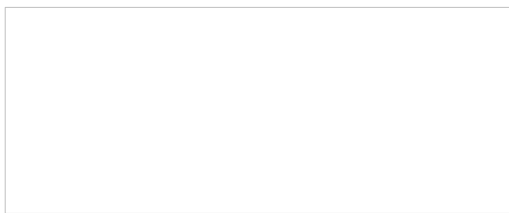


某邮储银行客户SR6608与MSR2600 IPSec对接失败的问题

傅昆 2014-12-08 发表

某邮储银行客户SR6608与MSR2600 IPSec对接失败的问题

一 组网:



二 问题描述:

2014年08月28日晚上11点左右,某邮储银行客户反映,SR6608(LNS)路由器下联的部分网点的MSR2600 IPSec无法建立。同时,MSR2600路由器IPSec可以连接J友商LNS。经过和客户反复沟通,确认邮储银行客户并没有对设备、网络做任何改动,MSR2600路由器突然无法和SR6608(LNS)路由器建立IPSec连接。

三 过程分析:

故障发生以后,由于业务的原因,客户不允许对核心设备SR6608做任何操作,先收集了MSR2600路由器的诊断信息和IPSec debug ike all信息。

从debug信息分析,MSR2600路由器发出IKE协商请求后没有收到对端SR6608路由器的应答报文:

*Dec 3 22:23:43:319 2014 QZ-FJJingMaoXXATM-2600-2 IKE/7/DEBUG: send message:

*Dec 3 22:23:43:319 2014 QZ-FJJingMaoXXATM-2600-2 IKE/7/DEBUG: ICOOKIE:

0x85b369867121e4f2

*Dec 3 22:23:43:319 2014 QZ-FJJingMaoXXATM-2600-2 IKE/7/DEBUG: RCOOKIE: **0x0000000000000000000000**

*Dec 3 22:23:43:320 2014 QZ-FJJingMaoXXATM-2600-2 IKE/7/DEBUG: NEXT_PAYLOAD: SA

*Dec 3 22:23:43:320 2014 QZ-FJJingMaoXXATM-2600-2 IKE/7/DEBUG: VERSION: 16

*Dec 3 22:23:43:320 2014 QZ-FJJingMaoXXATM-2600-2 IKE/7/DEBUG: EXCH_TYPE: AGGRESSIVE

*Dec 3 22:23:43:321 2014 QZ-FJJingMaoXXATM-2600-2 IKE/7/DEBUG: FLAGS: []

*Dec 3 22:23:43:321 2014 QZ-FJJingMaoXXATM-2600-2 IKE/7/DEBUG: MESSAGE_ID: 0x00000000

*Dec 3 22:23:43:321 2014 QZ-FJJingMaoXXATM-2600-2 IKE/7/DEBUG: LENGTH: 340

*Dec 3 22:23:43:321 2014 QZ-FJJingMaoXXATM-2600-2 IKE/7/DEBUG: exchange release: freeing exchange 9ee1bf0

通过和客户沟通,另外安排时间继续定位此问题,以便可以收集SR6608路由器的相关信息。

2014年08月29日晚上20点,收集了SR6608路由器的诊断和debug ike all信息,通过信息分析:

MSR2600路由器dialer2接口上使能了IPSec策略,dialer2接口路由的下一跳地址是LNS SR6608路由器的VT接口地址,IKE PEER指定的地址是SR6608路由器上VT接口地址。MSR2600路由器dialer2接口成功获取地址后,向SR6608路由器上VT接口地址发起IKE请求,结果SR6608路由器上IKE DEBUG信息显示“Failed to find IKE peer by address”,将MSR2600发送的IKE请求丢弃。丢弃该报文的原因是报文的入接口GE3/0/46并没有使能IPSec策略(为什么入接口GE3/0/46没有使能IPSec策略,报文却可以进入IKE流程处理呢?那是因为SR6608路由器上的VT接口使能了IPSec策略,所以报文能进入IKE流程处理)。

*Dec 4 21:44:38:870 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: received message:

*Dec 4 21:44:38:871 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: ICOOKIE: 0x8ce5b2187a296a0a

*Dec 4 21:44:38:872 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: RCOOKIE: 0x0000000000000000000000

*Dec 4 21:44:38:872 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: NEXT_PAYLOAD: SA

*Dec 4 21:44:38:873 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: VERSION: 16

*Dec 4 21:44:38:873 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: EXCH_TYPE: AGGRESSIVE

*Dec 4 21:44:38:874 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: FLAGS: []

*Dec 4 21:44:38:875 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: MESSAGE_ID: 0x00000000

*Dec 4 21:44:38:875 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: LENGTH: 340

*Dec 4 21:44:38:876 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: exchange lookup all list from COOKIE: iCOOKIE 8ce5b2187a296a0a

*Dec 4 21:44:38:876 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: parse payloads: payload SA

*Dec 4 21:44:38:877 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: parse payloads: payload KEY_EXCH

*Dec 4 21:44:38:877 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: parse payloads: payload NONCE

*Dec 4 21:44:38:878 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: parse payloads: payload CERT_RE

Q

*Dec 4 21:44:38:879 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: parse payloads: payload VENDOR
*Dec 4 21:44:38:879 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: parse payloads: payload ID
*Dec 4 21:44:38:880 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: validate payload SA
*Dec 4 21:44:38:880 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: DOI: 1
*Dec 4 21:44:38:881 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: receive DPD Protocol Vendor ID
*Dec 4 21:44:38:882 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: exchange setup(R): 12637870
*Dec 4 21:44:38:882 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: parse payloads: payload PROPOSAL
*Dec 4 21:44:38:883 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: parse payloads: payload TRANSFORM
*Dec 4 21:44:38:883 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: validate payload PROPOSAL
*Dec 4 21:44:38:884 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: NO: 1
*Dec 4 21:44:38:885 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: PROTO: ISAKMP
*Dec 4 21:44:38:885 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: SPI_SZ: 0
*Dec 4 21:44:38:886 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: NTRANSFORMS: 1
*Dec 4 21:44:38:886 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: validate payload TRANSFORM
*Dec 4 21:44:38:887 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: NO: 0
*Dec 4 21:44:38:888 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: ID: 1
*Dec 4 21:44:38:888 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: Transform 0's attributes
*Dec 4 21:44:38:889 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: Attribute ENCRYPTION_ALGORITHM : DES_CBC
*Dec 4 21:44:38:889 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: Attribute HASH_ALGORITHM : SHA
*Dec 4 21:44:38:890 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: Attribute AUTHENTICATION_METHOD : RSA_SIG
*Dec 4 21:44:38:891 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: Attribute GROUP_DESCRIPTION : MODP_1024
*Dec 4 21:44:38:891 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: Attribute LIFE_TYPE : SECONDS
*Dec 4 21:44:38:892 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: Attribute LIFE_DURATION : 604800
*Dec 4 21:44:38:892 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: validate payload KEY_EXCH
*Dec 4 21:44:38:893 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: validate payload ID
*Dec 4 21:44:38:894 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: TYPE: 9
*Dec 4 21:44:38:894 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: DOI_DATA: 0x000000
*Dec 4 21:44:38:895 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: id information: type 9 proto 0 port 0
*Dec 4 21:44:38:895 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: validate payload CERT_REQ
*Dec 4 21:44:38:896 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: TYPE: X509_SIG
*Dec 4 21:44:38:897 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: validate payload NONCE
*Dec 4 21:44:38:897 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: validate payload VENDOR
*Dec 4 21:44:38:898 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: vendor ID seen
*Dec 4 21:44:38:898 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: exchange check: checking for required SA
*Dec 4 21:44:38:899 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: exchange check: checking for required KEY_EXCH
*Dec 4 21:44:38:900 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: exchange check: checking for required NONCE
*Dec 4 21:44:38:900 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: exchange check: checking for required ID
*Dec 4 21:44:38:901 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: negotiate sa: transform 0 proto 1 proposal 1 compatible
*Dec 4 21:44:38:901 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: negotiate sa: proposal 1 succeeded
***Dec 4 21:44:38:902 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: P1 handle ID: Failed to find IKE peer by address.**

***Dec 4 21:44:38:903 2014 FJYC-LNS-SR6604-1 IKE/7/DEBUG: exchange state machine: Failed to receive message.**

MSR2600路由器上配置了NQA，会持续触发IKE请求，SR6608会收到同样的ICOOKIE重复请求报文，直接丢弃。

IKE/7/DEBUG: received message: dropping setup for existing SA.

后来，问题原因基本清楚了，和客户做了沟通。客户的LAC是放到运营商的，所以对LAC的改动客户并不知情。由于运营商LAC的配置改变，导致了SR6608路由器只做IPSec，而取消了LNS的功能，由于以前配置的IPSec策略是在VT口上的，因为导致此故障。

四 解决方法：

下面方法采用一个即可解决该问题：

- 1、修改SR6608的配置，把VT接口的IPSec策略使能到物理口GE3/0/46；
- 2、修改LAC的配置，把LNS指回SR6608，即让SR6608做IPSec over L2TP。