

某局点 MSR设备 L2TP over IPSEC隧道建立异常

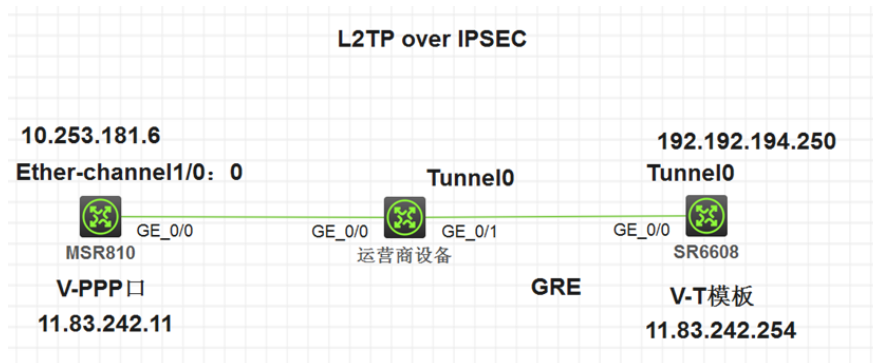
L2TP VPN

IPSec VPN

苏清秀

2020-02-21 发表

组网及说明



组网描述如下：

- (1) MSR810 (MSR810-LM-CNDE-SJK) -V7-R0707P16、SR6608-V7-R7740P20；
- (2) MSR810上面的V-PPP口与SR6608上面的V-T模板进行搭建L2TP隧道，MSR810上面的Ether-channel1/0:0口与SR6608上面的Tunnel口建立ipsec隧道，这里关于ipsec策略不下发到物理接口是因为联通运营商规定的，下发到物理接口不生效；
- (3) 运营商设备上面Tunnel口与SR6608上面的Tunnel口，建立GRE隧道；
- (4) MSR810与SR6608之间通过运营商专线连通的，所以Ether-channel1/0:0口地址是固定的。所以大致上就是MSR810与SR6608上面建立L2TP over IPSEC，运营商设备与SR6608上面建立GRE隧道。

问题描述

问题现象：

- (1) SR6608上面的V-T口物理/协议双down了？
- (2) MSR810上的V-PPP口无规律的持续性up/down，SR6608上面的V-A口无规律的持续性up/down。在SR6608上面ping 11.83.242.11是可以ping通的，反之在MSR810上面ping 11.83.242.254是不通的？此时dis l2tp tunnel、dis l2tp session、dis ike sa、dis ipsec sa 都是能够建立的；
- (3) ACL匹配失败？此时dis ike sa、dis ipsec sa查看不到表项了；
- (4) dis l2tp tunnel 无表项？在SR6608上面ping 11.83.242.11是可以ping通的，反之在MSR810上面ping 11.83.242.254是不通的。

过程分析

(1) V-T口双down是正常现象，V-A口必须是up的，不能是down的。L2TP会话建立之后，LNS需要创建一个VA（Virtual Access虚拟访问）接口用于和LAC交换数据。VA接口基于VT（Virtual Template，虚拟模板）接口上配置的参数动态创建。因此，配置LNS时需要首先创建VT接口，并配置该接口的参数。另外可以创建VA池，具体见配置和命令手册。

(2) 关于（2）个问题，见下面解决方案。

(3) ACL匹配问题，建议的是都配置成网段或者是主机地址，但是要“各自对应”，也就是说，确定好的分支和总部属于不通的ACL感兴趣流，不可以混。

(4) 可以开启debug看一下：

[11:15:33]The reason of dropping packet is encryption failed. //因为加密失败导致的ipsec协商不起来此时，两端的ipsec加密算法是一致的，都是国密算法（属于软加密）。不存在软件加密有问题的情况。

ike proposal 1

encryption-algorithm sm4-cbc

authentication-algorithm sm3

解决方法

(2) 解决方案是：先检查了两台设备的基本配置，没有问题。将V-T口和Tunnel接口视图下面配置了“service slot 3”命令后，不再出现接口持续up/down的问题了。一般情况下，设备在有很多逻辑接口，V-T口、tunnel接口的情况下，在堆叠之后，建议虚接口上配置service slot。选择的slot可以是与LAC相连的接口所在的单板。

指定2号成员设备的2号单板作为转发虚拟模板接口10下VA接口的流量的主用单板。（IRF模式）

<Sysname> system-view

[Sysname] interface virtual-template 10

[Sysname-Virtual-Template10] service chassis 2 slot 2

指定2号成员设备的2号槽位单板作为转发虚拟模板接口10下VA接口的流量主用单板，同时指定2号成员设备的3号槽位单板为备用单板。（IRF模式）

```
<Sysname> system-view
```

```
[Sysname] interface virtual-template 10
```

```
[Sysname-Virtual-Template10] service chassis 2 slot 2
```

```
[Sysname-Virtual-Template10] service standby chassis 2 slot 3
```

（4）后面查看设备的图片，发现设备没有多余的slot槽位，那就是在设备里面了。MSR810-LM-CNDE-SJK有自己的硬件加密卡，当设备启动运行的时候，先用自己的硬件加密卡进行加密，当加密的结果与软件加密的结果不一致的时候，就不能用了。

所以为了防止这种情况出现：需要在隐藏视图下，强制关闭硬件加密，之后就可以了。