V5防火墙路由下一跳配置错误导致L2TP VPN不通

L2TP 王林 2016-06-02 发表

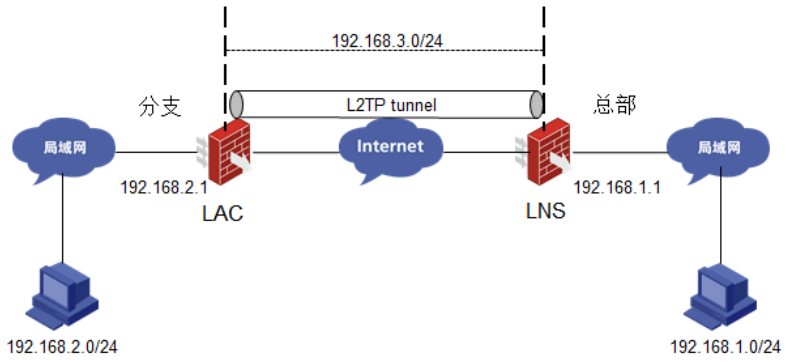

图1.1

分支用V5防火墙F100-C-G作为出口，采用PPPOE拨号方式上网，内网网段为192.168.2.0/24，网关192.168.2.1在防火墙上。总部用V5防火墙F100-M-SI作为出口，采用静态公网IP地址方式上网，内网网段为192.168.1.0/24，网关192.168.1.1在防火墙上。分支和总部采用LAC-Auto-Initiated模式建立L2TP VPN隧道，F100-C-G作LAC， F100-M-SI作LNS，隧道ip地址段为192.168.3.0/24,其中LAC的隧道接口（VT1）ip地址采用拨号获取，LNS隧道接口（VT0）ip地址为192.168.3.254，具体组网如上图1.1。目前内网互ping不通，并且也无法互相访问。

对于L2TP VPN无法通信的问题，一般排查步骤可分为三步：检查L2TP隧道是否成功建立，检查L2TP会话是否存在，路由配置和安全策略是否正确。

1.通过在LAC上查看L2TP隧道建立信息，发现存在对应的隧道，如下所示：

```
 display l2tp tunnel
    Total tunnel = 1
LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
     1       5       218.8.184.186    1701   1        H3C
```

2.检查是否存在对应的会话，通过在LAC上查看，会话也存在，并且LAC L2TP虚接口获取到的ip地址为192.168.3.108：

```
 display l2tp session
    Total session = 1
    LocalSID  RemoteSID  LocalTID
     6451      16286      1
```

3.L2TP隧道和会话都存在，说明内网无法互通肯定和路由以及安全策略有关。两端内网相互通信，涉及到的路径为：192.168.2.0/24——192.168.3.108（LNS分配给LAC VT1口的ip地址）——192.168.3.254(LNS VT0接口地址)——192.168.1.0/24，通过检查两端配置，并没有发现影响内网互通的安全策略存在，而且值得一提的是，通过两端互ping测试，发现LAC到LNS内网192.168.1.0/24可以ping通，但LNS无法ping通LAC内网192.168.2.0 /24，由于LNS和LAC的L2TP接口地址均属于两端的直连网段，所以原因就是LNS端到192.168.2.0/24的路由不正确,但是通过查看LNS的路由信息，并无异常，确实存在到192.168.2.0/24的正确路由表项，如下红色摘取部分：

```
display ip routing-table
Routing Tables: Public
       Destinations : 31       Routes : 31

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
192.168.2.0/24      Static 60   0           192.168.3.254   VT0
```

为了对比分析，这里我们把LAC端对应的正确路由也放到这里讨论：

```
  dis ip routing-table
Routing Tables: Public
       Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
192.168.1.0/24      Static 60   0           192.168.3.108   VT1
```

可以看到，两端的路由都是将下一跳指定为出接口，即VT接口，但为什么就会出现LAC端路由正确，

而LNS端路由错误呢?

最后，通过在LNS端查询L2TP隧道信息，发现存在多个L2TP隧道，也就是说LNS和多个LAC建立了L2TP VPN，如果将到192.168.2.0网段的下一跳指定为LNS端隧道出接口，由于存在多个隧道，设备无法得知目的地址为192.168.2.0/24的数据包应该如何封装L2TP头部，也就不知道目的公网地址是多少，192.168.2.0/24网段的数据包无法从一个具体的隧道路由出去。另外这里不得不多说一句，到其他几个隧道的数据包之所以转发正常，是因为其他几个点L2TP VPN采用Client-Initiated模式，内网PC直接和LNS建立L2TP隧道，在LNS端上存在对应的直连路由。

LAC的L2TP虚接口，即VT1接口配置静态ip地址192.168.3.108，并且在LNS端，修改到192.168.2.0/24网段的路由，将其下一跳指定为192.168.3.108。

V5防火墙使用LAC-Auto-Initiated模式建立L2TP VPN隧道时，最好把到对端内网路由的下一跳指定为对端的L2TP接口地址，不要指定成本端的L2TP接口地址，以免当存在多个隧道时，路由出错。