中低端防火墙点到多点GRE over IPsec模式下Tunnel口无法ping通对端问题

L2TP over IPSec VP　GRE VPN　孔凡安　2024-02-22 发表

组网及说明

点到多点GRE over IPsec，类似于下面。总部对接多个分支：

告警信息

不涉及

问题描述

现场分支需求如下：
分支防火墙DNS解析的流量需要走GRE over IPsec隧道到总部防火墙处DNS服务器解析，但是域名解析均是失败的。

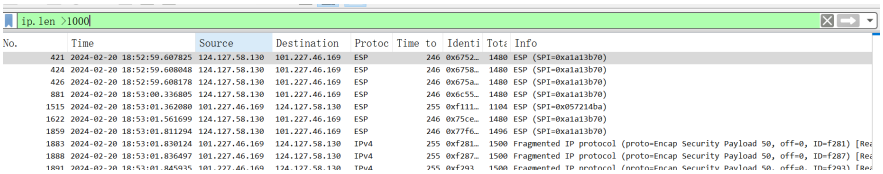
进一步测试发现Tunnel口互ping均不通。

过程分析

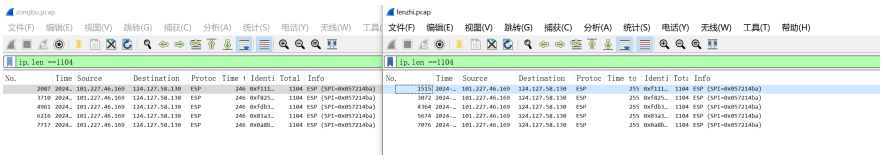
针对此类问题，先看两边是否有对应的IPsec SA和IKE SA。现场均是存在的。如果隧道成功建立的话问题排查相对简单。
分支ping总部的情况下，分支会话有发无收，总部会话收发正常；总部ping分支的话，总部会话有发无收，分支会话无。

基于以上简单的小测试，怀疑问题可能出现在总部，可能是总部没有将封装后的ESP报文发送出去。
于是两边一起抓包对比，需要注意的是，GRE over IPsec的场景下，Tunnel口互ping的流量经过封装后，源目地址变为两边的IPsec网关地址。因此抓包的acl需要书写正确。此外，经过IPsec封装后，ESP报文是加密的并非明文显示，需要我们在ping的时候固定ICMP报文的字节大小与数量，方便在海量的ESP报文里定位到我们需要的报文。

测试条件为：分支ping总部，ping 1000字节，5个报文。
分支侧抓包并过滤如下：



看起来并不好查看那个是ICMP报文封装后的ESP报文，本地发出TTL一般是255，封装后字节大小加上100多也差不多，于是锁定ip.length == 1104并进行过滤如下：



可以看出，分支（文件名fenzhi.pcap）发出5个ESP报文，总部（文件名zongbu.pcap）收到5个。因此问题确认出现在总部没有回应。
于是对总部的内层流量debug分析，可以参考案例：某局点IPsec中心模板方式运行中故障典型分析

debug没有发现丢包，且报文已经送往Tunnel口：

> [20240220_16:50:38]*Feb 20 16:50:30:620 2024 BJ-ZY-A3-2F-FW-01&02 IPFW/7/IPFW_PACKET: -COntext=1-Slot=1;
> [20240220_16:50:38]Sending, interface = Tunnel0
> [20240220_16:50:38]version = 4, headlen = 20, tos = 0
> [20240220_16:50:38]pktlen = 84, pktid = 31405, offset = 0, ttl = 255, protocol = 1
> [20240220_16:50:38]checksum = 30029, s = 10.3.91.214, d = 10.3.91.210
> [20240220_16:50:38]channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
> [20240220_16:50:38]VsysID = 1

> [20240220_16:50:38]prompt: Sending IP packet from local at interface Tunnel0.
> [20240220_16:50:38]Payload: ICMP
> [20240220_16:50:38] type = 0, code = 0, checksum = 0x9967.

排查到这，问题陷入僵局。总部为何没有封装报文并发出呢?
和现场了解到其他分支也存在同样情况，一线展示了下分支带接口地址可以ping通总部。感觉还是和现场配置有关。

解决方法

后续查看总部配置发现GRE P2MP隧道的映射表项只有对应接口网段，不包含dns服务器以及Tunnel口映射的表项。
添加DNS服务器地址到映射表项后，问题解决。
对应命令:

map命令用来配置GRE P2MP隧道的映射表项。

undo map命令用来删除GRE P2MP隧道的映射表项。

【命令】

map [**vpn-instance** *vpn-instance-name*] **branch-network-address** *branch-network-address* { *mask* | *mask-length* } **tunnel-destination** *tunnel-dest-address* [**checksum-fill** *checksum-value*]

undo map [**vpn-instance** *vpn-instance-name*] **branch-network-address** *branch-network-address* { *mask* | *mask-length* } [**tunnel-destination** *tunnel-dest-address*]

【缺省情况】

未配置GRE P2MP隧道的映射表项。

【视图】

GRE P2MP隧道模板视图

【缺省用户角色】

network-admin
mdc-admin

【参数】

vpn-instance *vpn-instance-name*：分支网络所属的VPN实例。*vpn-instance-name*表示MPLS L3VPN的VPN实例名称，为1～31个字符的字符串，区分大小写。如果未指定本参数，则表示该分支网络属于公网。

branch-network-address *branch-network-address*：分支网络的IPv4地址。

mask：分支内网络IPv4地址的掩码，为点分十进制格式。

mask-length：分支内网IPv4地址的掩码长度，取值范围为0～32。

tunnel-destination *tunnel-dest-address*：GRE P2MP隧道的目的IPv4地址。

checksum-fill *checksum-value*：填充的IPv4地址，为点分十进制格式。当指定本参数时，在GRE头中的checksum字段中携带该值，如果未指定本参数，则不对GRE头中的checksum字段进行填充。

【使用指导】

非缺省vSystem不支持本命令。

一个GRE P2MP隧道模板视图下可以配置多个GRE P2MP隧道的映射表项，每个表项定义了一个分支网络地址及其所属的VPN与所属隧道目的地址的对应关系，该对应关系是唯一的，即同一个分支网络地址不能对应不同的隧道目的地址。

如果分支网络地址为私网地址，则需要指定私网地址所属的VPN。

在某些特殊应用场景，分支网络中存在虚拟机，并且虚拟机下挂多个用户，为保证数据报文能够发送到用户，需要通过配置的**checksum-fill**参数填充IPv4地址至checksum字段中，当分支网络接收到GRE报文后，会再根据checksum字段中的IPv4地址将数据报文转发到指定的虚拟主机上。因此，请结合实际组网要求准确使用**checksum-fill**参数，不当使用会导致GRE报文校验失败。

【举例】

在GRE P2MP隧道模板aa视图下，配置一条映射表项，分支网络地址为192.168.0.11，掩码长度为32，隧道目的地址为10.108.113.71，填充的IPv4地址为192.168.20.1。

```
<Sysname> system-view
[Sysname] gre p2mp-template aa
[Sysname-p2mp-template-aa] map branch-network-address 192.168.0.11 32 tunnel-destination
10.108.113.71 checksum-fill 192.168.20.1
```

【相关命令】

- **gre p2mp-template(system view)**