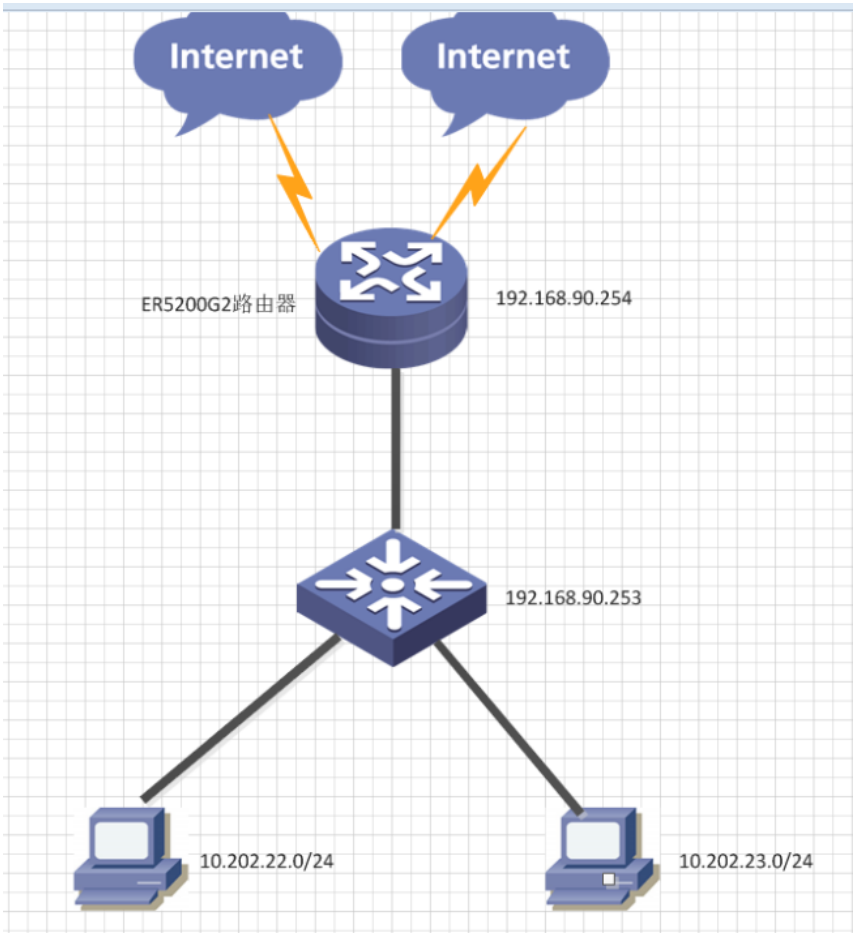
ER5200G2 ipsec隧道建立但是不通故障经验案例

IPSec VPN　单畅　2018-09-26 发表

组网及说明



拓扑：

ER5200G2 WAN2（117.158.45.108）-------（116.228.72.155）对端设备

私网数据流：

10.202.22.0/24（以及10.202.23.0/24）--------192.168.100.0/24

问题描述

隧道已经建立，但是私网ping不通。而且本端终端tracert 192.168.100.0测试发现，10.202.22.0网段终端的数据流到ER设备上后，没有匹配ipsec隧道接口出去，而是跑到公网上了，截图可以看到有很多公网地址。

名称	方向	隧道两端	AH SPI	AH 算法	ESP SPI	ESP 算法	数据流
sfl2	in	116.228.72.155 =>117.158.45.108	----	----	0x4ef719da	3DES_MD5	192.168.100.0/24 =>10.202.23.0/24
sfl2	out	117.158.45.108 =>116.228.72.155	----	----	0x773e7ac4	3DES_MD5	10.202.23.0/24 =>192.168.100.0/24
nh2	in	180.153.139.66 =>117.158.45.108	----	----	0x4ef719db	3DES_MD5	10.4.0.0/24 =>10.202.23.0/24
nh2	out	117.158.45.108 =>180.153.139.66	----	----	0x1701eba	3DES_MD5	10.202.23.0/24 =>10.4.0.0/24
nh1	in	180.153.139.66 =>117.158.45.108	----	----	0x4ef719dc	3DES_MD5	10.4.0.0/24 =>10.202.22.0/24
nh1	out	117.158.45.108 =>180.153.139.66	----	----	0xadd8008c	3DES_MD5	10.202.22.0/24 =>10.4.0.0/24
sfl	in	116.228.72.155 =>117.158.45.108	----	----	0x4ef719f0	3DES_MD5	192.168.100.0/24 =>10.202.22.0/24
sfl	out	117.158.45.108 =>116.228.72.155	----	----	0x2a358711	3DES_MD5	10.202.22.0/24 =>192.168.100.0/24

第 1 页/共 1 页 共 8 条记录 每页 10

Tracert发现没有匹配ipsec隧道，而是上到公网了：

```
C:\Windows\system32>tracert 192.168.100.1

通过最多 30 个跃点跟踪到 192.168.100.1 的路由

  1    29 ms     5 ms     4 ms  10.202.23.254
  2    <1 毫秒   <1 毫秒   <1 毫秒 192.168.90.254
  3     3 ms     2 ms     2 ms  117.158.45.97
  4     3 ms     3 ms     3 ms  111.5.71.33
  5     2 ms     3 ms     2 ms  221.176.98.238
  6    11 ms    17 ms     6 ms  221.176.99.13
  7     *        7 ms     7 ms  221.183.13.29
  8    27 ms    27 ms    27 ms  221.183.36.145
  9    38 ms    28 ms    28 ms  221.176.18.234
 10    28 ms    31 ms    28 ms  221.176.24.86
 11    42 ms    43 ms    42 ms  221.176.24.89
 12     *        *        *     请求超时。
 13     *        *        *     请求超时。
 14     *        *        *     请求超时。
 15     *        *        *     请求超时。
 16
```

过程分析

查看配置没有发现问题：

看ipsec配置以及路由配置都没有问题。继续看设备上别的部分配置，发现现场除了路由外还添加了策略路由的配置，而策略路由中将内网网段10.202.22.0/24以及10.202.23.0/24的流量重定向到了WAN2口，由于策略路由优先级比静态路由高，因此内网终端访问对端私网地址的时候流量没有走ipsec隧道而是从公网出去，导致不通。

解决方法

将策略路由删掉。