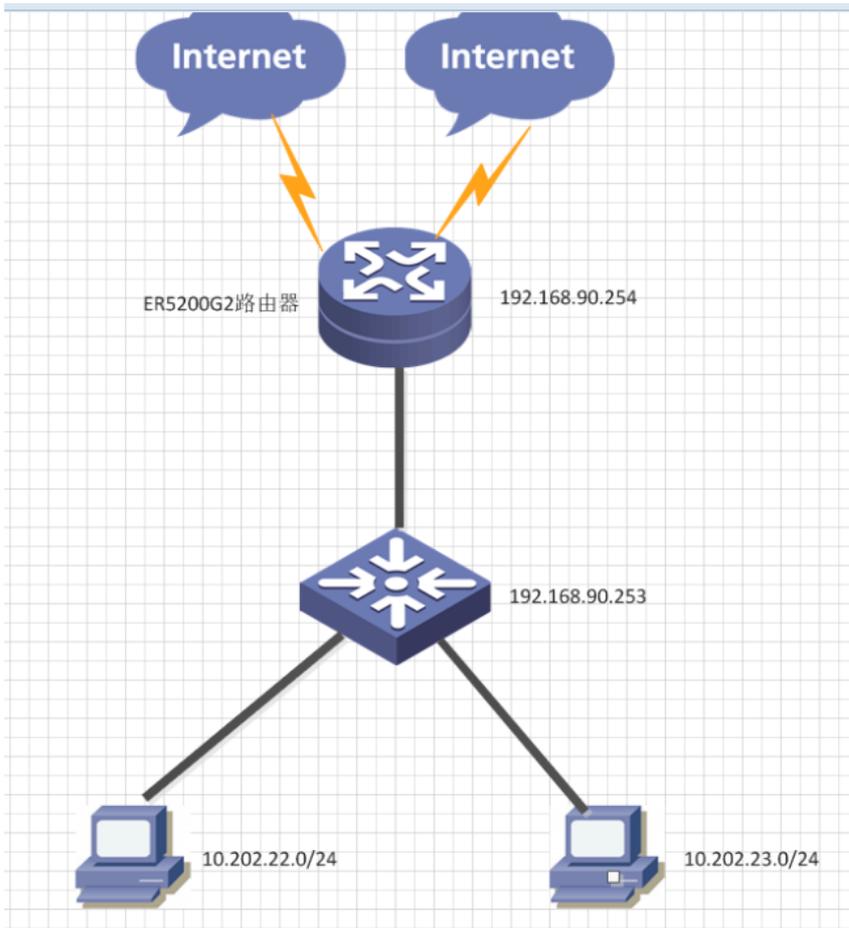


组网及说明



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

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    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:

安全联盟 | 虚接口 | **IKE安全提议** | IKE对等体 | IPsec安全提议 | IPsec安全策略

**虚接口**

虚接口的配置修改后, 需要重新启用(先禁用再启用)引用该虚接口的IPsec安全策略或重新使能IPSEC功能, 新的配置才能生效。

关键字: [名称] [查询] [显示全部]

操作	序号	名称	绑定接口	描述
	1	ipsec0	WAN2	
	2	ipsec1	WAN2	

第 1 页 / 共 1 页 共 2 条记录 每页 10 行 << 1 >> Go >>>

安全联盟 | 虚接口 | **安全提议** | IKE对等体 | IPsec安全提议 | IPsec安全策略

**安全提议**

安全提议的配置修改后, 需要重新启用(先禁用再启用)引用该安全提议的IPsec安全策略或重新使能IPSEC功能, 新的配置才能生效。

关键字: [名称] [查询] [显示全部]

操作	序号	名称	认证算法	加密算法	DH组
	1	sfl	MD5	3DES	DH2 modp1024

第 1 页 / 共 1 页 共 1 条记录 每页 10 行 << 1 >> Go >>>

安全联盟 | 虚接口 | **IKE安全提议** | **IKE对等体** | IPsec安全提议 | IPsec安全策略

**IKE对等体**

IKE对等体的配置修改后, 需要重新启用(先禁用再启用)引用该对等体的IPsec安全策略或重新使能IPSEC功能, 新的配置才能生效。

关键字: [名称] [查询] [显示全部]

操作	序号	名称	虚接口	对端地址	模式	ID类型	安全提议	DPD
	1	sfl	ipsec0	116.228.72.155	主模式	----	sfl	关闭
	2	nh	ipsec1	180.153.139.66	主模式	----	sfl	关闭

第 1 页 / 共 1 页 共 2 条记录 每页 10 行 << 1 >> Go >>>

安全联盟 | 虚接口 | **IKE安全提议** | **IKE对等体** | **IPsec安全提议** | IPsec安全策略

**IPsec安全提议**

IPsec安全提议的配置修改后, 需要重新启用(先禁用再启用)引用该安全提议的IPsec安全策略或重新使能IPSEC功能, 新的配置才能生效。

关键字: [名称] [查询] [显示全部]

操作	序号	名称	安全协议	AH算法	ESP算法
	1	sfl	ESP	----	3DES-MD5

第 1 页 / 共 1 页 共 1 条记录 每页 10 行 << 1 >> Go >>>

安全联盟 虚接口 **IKE安全提议** **IKE对等体** **IPSec安全提议** **IPSec安全策略**

**IPSec设置**

启用IPSec功能  
应用

**安全策略**

虚接口、IKE安全提议、IKE对等体和IPSec安全提议的配置都修改完成后，只需要重新启用(先禁用再启用)相关的IPSEC安全策略一次或重新启用IPSEC功能一次，新的配置就能生效；另外，修改IPSEC安全策略的配置也能使新的配置生效。

关键字: 名称  查询 显示全部

操作	序号	名称	状态	本端子网段	对端子网段	协商类型	其它
	1	sfl	启用	10.202.22.0/255.255.255.0	192.168.100.0/255.255.255.0	IKE协商	对等体: sfl
	2	sfl2	启用	10.202.23.0/255.255.255.0	192.168.100.0/255.255.255.0	IKE协商	对等体: sfl
	3	nh1	启用	10.202.22.0/255.255.255.0	10.4.0.0/255.255.255.0	IKE协商	对等体: nh
	4	nh2	启用	10.202.23.0/255.255.255.0	10.4.0.0/255.255.255.0	IKE协商	对等体: nh

第 1 页/共 1 页 共 4 条记录 每页 5 行 1 Go

序号	目的地址	子网掩码	下一跳地址	出接口
1	10.4.0.0	255.255.255.0		ipsec1
2	10.202.22.0	255.255.255.0	192.168.90.253	VLAN1
3	10.202.23.0	255.255.255.0	192.168.90.253	VLAN1
4	192.168.100.0	255.255.255.0		ipsec0
5	211.138.24.66	255.255.255.255	117.159.193.193	WAN1
6	211.138.30.66	255.255.255.255	117.159.193.193	WAN1
7	222.85.85.85	255.255.255.255	117.158.45.97	WAN2
8	0.0.0.0	0.0.0.0	117.159.193.193	WAN1
9	0.0.0.0	0.0.0.0	117.158.45.97	WAN2

刷新



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。

静态路由 **策略路由**

**策略路由表**

关键字: 描述  查询 显示全部

操作	序号	协议类型	源端口号	源IP地址段	目的端口号	目的IP地址段	生效时间	出接口	状态	强制	描述
----	----	------	------	--------	-------	---------	------	-----	----	----	----

第 1 页/共 1 页 共 0 条记录 每页 8 行 1 Go