

# MSR3640路由器映射ssl vpn服务不成功经验案例

NAT SSL VPN GRE VPN 孙兆强 2019-07-25 发表

## 组网及说明



防火墙在内网提供ssl vpn服务，MSR3640做nat server映射ssl vpn端口。

## 问题描述

现场pc连接公网拨ssl vpn正常，客户移动定制平板通过4G网络无法拨成功。

## 过程分析

### 1、查看路由器nat server配置

nat server protocol tcp global 117.187.64.xx 6633 inside 10.10.112.21 443

PC能拨号成功说明MSR3640映射配置及FW的ssl vpn配置均没问题。

2、移动平板拨号时在路由器上查看nat会话dis nat session destination-ip 117.187.64.xx verbose无任何会话信息，且FW上未抓包任何相关报文。pc拨号时有nat会话。怀疑是移动平板拨号时报文没发到路由器。

3、移动平板拨号时接口抓包查看，报文已发过来，但从报文结构看，移动平板是先与MSR3640路由器建立GRE，拨ssl vpn的流量封装在GRE里面。

390	1.624599	10.68.98.21	117.187.64.54	TCP	90	55700	-	6633	[SYN]	Seq=0	Min=65535	Len=0	MSS=1360	SACK_PERM=1	TSval=6893126	TSecr=0	WS=256	
391	1.624609	117.187.64.54	10.68.98.21	TCP	90	6633	-	55700	[ACK]	Seq=0	Min=65535	Len=0	MSS=1350	WS=8	SACK_PERM=1	TSval=78177521	TSecr=6893126	
416	1.749756	10.68.98.21	117.187.64.54	TCP	90	55700	-	6633	[ACK]	Seq=1	Min=81664	Len=0	TSval=6893139	TSecr=78177521				
422	1.764388	10.68.98.21	117.187.64.54	TCP	244	55700	-	6633	[PSH, ACK]	Seq=1	Min=81664	Len=154	TSval=6893139	TSecr=78177521			[TCP segment of a reassembled PDU]	
423	1.764392	117.187.64.54	10.68.98.21	TCP	90	6633	-	55700	[ACK]	Seq=9	Min=65408	Len=0	TSval=78177660	TSecr=6893139				
444	1.864404	10.68.98.21	117.187.64.54	TCP	90	55700	-	6633	[ACK]	Seq=155	Min=81664	Len=0	TSval=6893149	TSecr=78177646				
445	1.864413	10.68.98.21	117.187.64.54	TCP	90	55700	-	6633	[ACK]	Seq=155	Min=81664	Len=0	TSval=6893149	TSecr=78177646				
446	1.864497	10.68.98.21	117.187.64.54	TCP	90	55701	-	6633	[SYN]	Seq=0	Min=65535	Len=0	MSS=1360	SACK_PERM=1	TSval=6893150	TSecr=0	WS=256	
447	1.864516	117.187.64.54	10.68.98.21	TCP	90	6633	-	55701	[ACK]	Seq=0	Min=65535	Len=0	MSS=1350	WS=8	SACK_PERM=1	TSval=78177761	TSecr=6893150	
454	1.899511	10.68.98.21	117.187.64.54	TCP	78	55700	-	6633	[RST]	Seq=155	Min=0	Len=0						
472	1.994330	10.68.98.21	183.192.192.163	TCP	98	[TCP Retransmission]	40495	-	8080	[SYN]	Seq=0	Min=65535	Len=0	MSS=1360	SACK_PERM=1	TSval=6893163	TSecr=0	WS=256
473	1.994334	10.68.98.21	183.192.192.163	TCP	78	[TCP Retransmission]	40495	-	8080	[SYN]	Seq=0	Min=65535	Len=0	MSS=1350	SACK_PERM=1	TSval=6893163	TSecr=0	WS=256

第一个SYN报文展开如下，内层目的地址和外层目的地址相同，均为路由器公网口地址。

```
Frame 390: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Hangzhou_bf:97:3b (d4:61:fe:bf:97:3b), Dst: Hangzhou_41:5e:5b (00:0f:e2:41:5e:5b)
Internet Protocol Version 4, Src: 221.177.232.229, Dst: 117.187.64.54
Generic Routing Encapsulation (IP)
Internet Protocol Version 4, Src: 10.68.98.21, Dst: 117.187.64.54
Transmission Control Protocol, Src Port: 55700, Dst Port: 6633, Seq: 0, Len: 0
```

有TCP协商和重传报文且无nat会话，说明路由器公网口nat没生效，路由器回复了tcp协商报文。

4、路由的处理逻辑是，在公网口对报文只做一次处理，先处理GRE封装，nat server没生效。GRE封装后内层报文在Tunnel口处理。

## 解决方法

在路由器GRE的Tunnel口做nat server

nat server protocol tcp global 117.187.64.xx 6633 inside 10.10.112.21 443