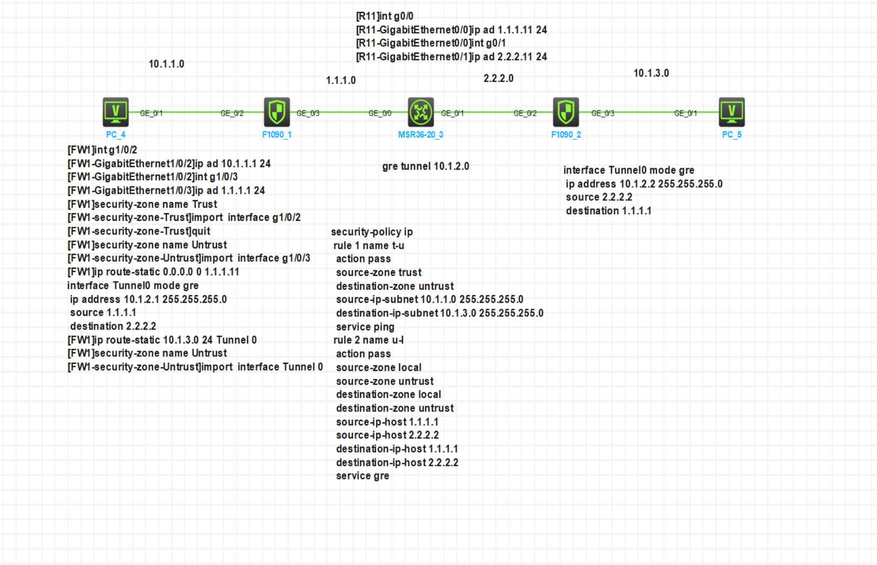
GRE相关实验

GRE VPN　IPSec VPN　**zhiliao_SB2b9b**　2024-08-28 发表

组网及说明



```
[R11]int g0/0
[R11-GigabitEthernet0/0]ip ad 1.1.1.11 24
[R11-GigabitEthernet0/0]int g0/1
[R11-GigabitEthernet0/1]ip ad 2.2.2.11 24
```

```
[FW1]int g1/0/2
[FW1-GigabitEthernet1/0/2]ip ad 10.1.1.1 24
[FW1-GigabitEthernet1/0/2]int g1/0/3
[FW1-GigabitEthernet1/0/3]ip ad 1.1.1.1 24
[FW1]security-zone name Trust
[FW1-security-zone-Trust]import  interface g1/0/2
[FW1-security-zone-Trust]quit
[FW1]security-zone name Untrust
[FW1-security-zone-Untrust]import  interface g1/0/3
[FW1]ip route-static 0.0.0.0 0 1.1.1.11
interface Tunnel0 mode gre
 ip address 10.1.2.1 255.255.255.0
 source 1.1.1.1
 destination 2.2.2.2
[FW1]ip route-static 10.1.3.0 24 Tunnel 0
[FW1]security-zone name Untrust
[FW1-security-zone-Untrust]import  interface Tunnel 0
```

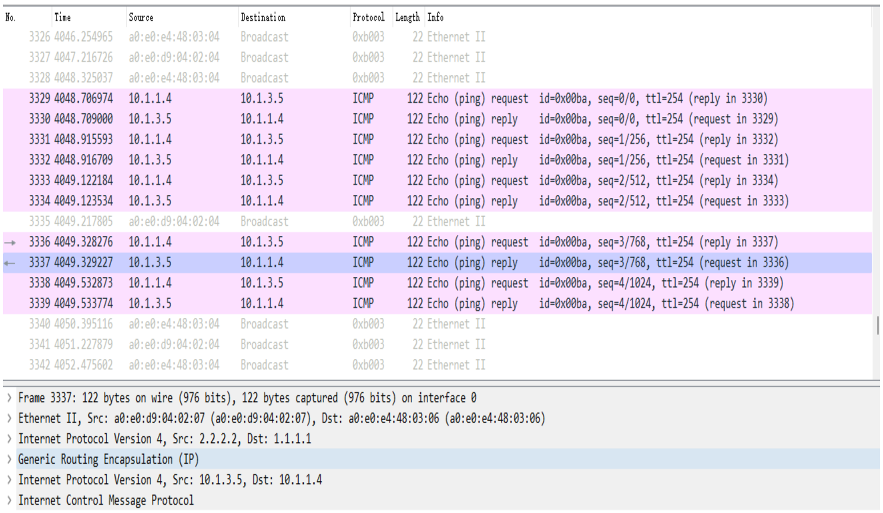
```
security-policy ip
 rule 1 name t-u
  action pass
  source-zone trust
  destination-zone untrust
  source-ip-subnet 10.1.1.0 255.255.255.0
  destination-ip-subnet 10.1.3.0 255.255.255.0
  service ping
 rule 2 name u-l
  action pass
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  source-ip-host 1.1.1.1
  source-ip-host 2.2.2.2
  destination-ip-host 1.1.1.1
  destination-ip-host 2.2.2.2
  service gre
```

```
interface Tunnel0 mode gre
 ip address 10.1.2.2 255.255.255.0
 source 2.2.2.2
 destination 1.1.1.1
```

问题描述

gre相关实验

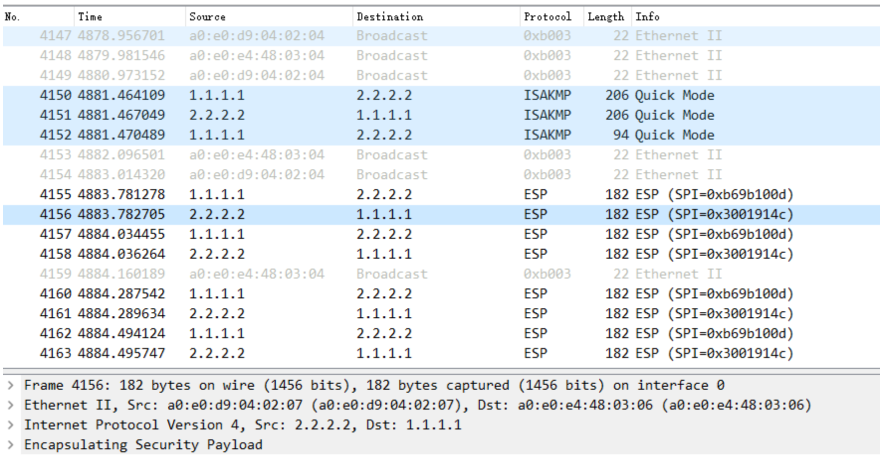
gre vpn配置完成后，在防火墙上能够看到相关会话协议为gre，抓包也能够看到报文进行了gre的封装，但是抓包显示的源目地址依然是报文的真实地址，而不是隧道地址，这是模拟器的bug吗？



```
No.       Time          Source              Destination         Protocol Length Info
    3326 4046.254965  a0:e0:e4:48:03:04   Broadcast           0xb003     22 Ethernet II
    3327 4047.216726  a0:e0:d9:04:02:04   Broadcast           0xb003     22 Ethernet II
    3328 4048.325037  a0:e0:e4:48:03:04   Broadcast           0xb003     22 Ethernet II
    3329 4048.706974  10.1.1.4            10.1.3.5            ICMP      122 Echo (ping) request  id=0x00ba, seq=0/0, ttl=254 (reply in 3330)
    3330 4048.709000  10.1.3.5            10.1.1.4            ICMP      122 Echo (ping) reply    id=0x00ba, seq=0/0, ttl=254 (request in 3329)
    3331 4048.915593  10.1.1.4            10.1.3.5            ICMP      122 Echo (ping) request  id=0x00ba, seq=1/256, ttl=254 (reply in 3332)
    3332 4048.916709  10.1.3.5            10.1.1.4            ICMP      122 Echo (ping) reply    id=0x00ba, seq=1/256, ttl=254 (request in 3331)
    3333 4049.122184  10.1.1.4            10.1.3.5            ICMP      122 Echo (ping) request  id=0x00ba, seq=2/512, ttl=254 (reply in 3334)
    3334 4049.123534  10.1.3.5            10.1.1.4            ICMP      122 Echo (ping) reply    id=0x00ba, seq=2/512, ttl=254 (request in 3333)
    3335 4049.217805  a0:e0:d9:04:02:04   Broadcast           0xb003     22 Ethernet II
→   3336 4049.328276  10.1.1.4            10.1.3.5            ICMP      122 Echo (ping) request  id=0x00ba, seq=3/768, ttl=254 (reply in 3337)
←   3337 4049.329227  10.1.3.5            10.1.1.4            ICMP      122 Echo (ping) reply    id=0x00ba, seq=3/768, ttl=254 (request in 3336)
    3338 4049.532873  10.1.1.4            10.1.3.5            ICMP      122 Echo (ping) request  id=0x00ba, seq=4/1024, ttl=254 (reply in 3339)
    3339 4049.533774  10.1.3.5            10.1.1.4            ICMP      122 Echo (ping) reply    id=0x00ba, seq=4/1024, ttl=254 (request in 3338)
    3340 4050.395116  a0:e0:e4:48:03:04   Broadcast           0xb003     22 Ethernet II
    3341 4051.227879  a0:e0:d9:04:02:04   Broadcast           0xb003     22 Ethernet II
    3342 4052.475602  a0:e0:e4:48:03:04   Broadcast           0xb003     22 Ethernet II

> Frame 3337: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
> Ethernet II, Src: a0:e0:d9:04:02:07 (a0:e0:d9:04:02:07), Dst: a0:e0:e4:48:03:06 (a0:e0:e4:48:03:06)
> Internet Protocol Version 4, Src: 2.2.2.2, Dst: 1.1.1.1
> Generic Routing Encapsulation (IP)
> Internet Protocol Version 4, Src: 10.1.3.5, Dst: 10.1.1.4
> Internet Control Message Protocol
```

gre over ipsec vpn配置完成后，在防火墙上能够看到相关会话协议为gre，ike sa和ipsec sa都建立成功，抓包能够看到隧道建立成功的过程以及报文经过了ipsec的封装，但是并未看出经过了gre的封装，从哪里可以体现出经过了gre的封装呢



```
No.       Time          Source              Destination         Protocol  Length Info
     4147 4878.956701   a0:e0:d9:04:02:04   Broadcast           0xb003       22 Ethernet II
     4148 4879.981546   a0:e0:e4:48:03:04   Broadcast           0xb003       22 Ethernet II
     4149 4880.973152   a0:e0:d9:04:02:04   Broadcast           0xb003       22 Ethernet II
     4150 4881.464109   1.1.1.1             2.2.2.2             ISAKMP      206 Quick Mode
     4151 4881.467049   2.2.2.2             1.1.1.1             ISAKMP      206 Quick Mode
     4152 4881.470489   1.1.1.1             2.2.2.2             ISAKMP       94 Quick Mode
     4153 4882.096501   a0:e0:e4:48:03:04   Broadcast           0xb003       22 Ethernet II
     4154 4883.014320   a0:e0:d9:04:02:04   Broadcast           0xb003       22 Ethernet II
     4155 4883.781278   1.1.1.1             2.2.2.2             ESP         182 ESP (SPI=0xb69b100d)
     4156 4883.782705   2.2.2.2             1.1.1.1             ESP         182 ESP (SPI=0x3001914c)
     4157 4884.034455   1.1.1.1             2.2.2.2             ESP         182 ESP (SPI=0xb69b100d)
     4158 4884.036264   2.2.2.2             1.1.1.1             ESP         182 ESP (SPI=0x3001914c)
     4159 4884.160189   a0:e0:e4:48:03:04   Broadcast           0xb003       22 Ethernet II
     4160 4884.287542   1.1.1.1             2.2.2.2             ESP         182 ESP (SPI=0xb69b100d)
     4161 4884.289634   2.2.2.2             1.1.1.1             ESP         182 ESP (SPI=0x3001914c)
     4162 4884.494124   1.1.1.1             2.2.2.2             ESP         182 ESP (SPI=0xb69b100d)
     4163 4884.495747   2.2.2.2             1.1.1.1             ESP         182 ESP (SPI=0x3001914c)

> Frame 4156: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface 0
> Ethernet II, Src: a0:e0:d9:04:02:07 (a0:e0:d9:04:02:07), Dst: a0:e0:e4:48:03:06 (a0:e0:e4:48:03:06)
> Internet Protocol Version 4, Src: 2.2.2.2, Dst: 1.1.1.1
> Encapsulating Security Payload
```

过程分析

接口ip地址、加入安全区域等基本配置略

gre vpn配置见图

gre over ipsec vpn配置：

```
#
interface GigabitEthernet1/0/3
 port link-mode route
 combo enable copper
 ip address 1.1.1.1 255.255.255.0
 ipsec apply policy map1
#
interface Tunnel0 mode gre
 ip address 10.1.2.1 255.255.255.0
 source 1.1.1.1
 destination 2.2.2.2
#
 ip route-static 0.0.0.0 0 1.1.1.11
 ip route-static 10.1.3.0 24 Tunnel0
#
acl number 3000
 rule 5 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
#
ipsec transform-set tran1
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec policy map1 10 isakmp
 transform-set tran1
 security acl 3000
 local-address 1.1.1.1
 remote-address 2.2.2.2
 ikev2-profile pro2  或ike-profile pro1
#
ike profile pro1
 keychain key1
 match remote identity address 2.2.2.2 255.255.255.0
#
ike keychain key1
 pre-shared-key address 2.2.2.2 255.255.255.0 key cipher $c$3$o5S+Sufy7JBH4G+gsqNnaX+gRFZYng==
#
ikev2 keychain key2
 peer p1
  address 2.2.2.2 255.255.255.0
  identity address 2.2.2.2
  pre-shared-key ciphertext $c$3$5+EbbPxS8gTHmzuZmcDStotMBFOR0Q==
#
ikev2 profile pro2
```

```
 authentication-method local pre-share
 authentication-method remote pre-share
 keychain key2
 match remote identity address 2.2.2.2 255.255.255.0
#
security-policy ip
 rule 1 name t-u
  action pass
  source-zone trust
  destination-zone untrust
  source-ip-subnet 10.1.1.0 255.255.255.0
  destination-ip-subnet 10.1.3.0 255.255.255.0
  service ping
 rule 2 name u-l
  action pass
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  source-ip-host 1.1.1.1
  source-ip-host 2.2.2.2
  destination-ip-host 1.1.1.1
  destination-ip-host 2.2.2.2
  service ipsec-ah
  service ipsec-esp
  service gre
#
```

采用ikev1或者ikev2都可以，能够看到ike sa/ikev2 sa和IPSec sa能够建立成功

解决方法

1