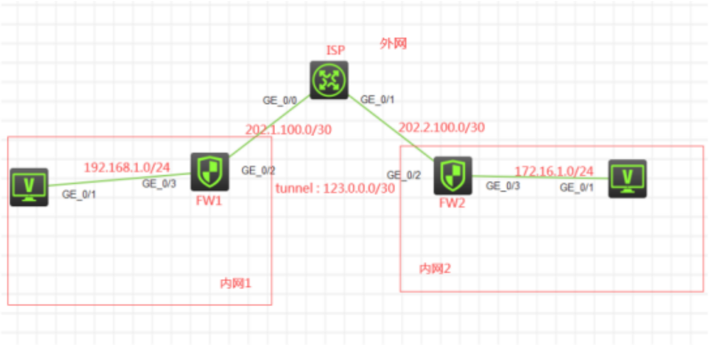
F1060 GRE VPN典型组网配置案例

GRE VPN H3C模拟器 韦家宁 2020-02-28 发表

组网及说明



组网说明：

本案例采用H3C HCL模拟器的F1060来模拟GRE VPN典型组网配置。内网和外网在网络拓扑图中已经有了明确的标识。FW1与FW2分别为各自内网的出口设备，提供NAT地址转换的服务。为了内网1和内网2能穿越NAT及外网进行通信，因此采用GRE VPN来实现。

配置步骤

1、按照网络拓扑图正确配置IP地址

2、FW1配置NAT，并配置默认路由指向ISP

3、FW2配置NAT，并配置默认路由指向ISP

4、FW1与FW2建立GRE VPN隧道

配置关键点

第一阶段调试（基础网络配置）：

ISP：

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname ISP
[ISP]int gi 0/0
[ISP-GigabitEthernet0/0]des <connect to FW1>
[ISP-GigabitEthernet0/0]ip address 202.1.100.1 30
[ISP-GigabitEthernet0/0]quit
[ISP]int gi 0/1
[ISP-GigabitEthernet0/1]des <connect to FW2>
[ISP-GigabitEthernet0/1]ip address 202.2.100.1 30
[ISP-GigabitEthernet0/1]quit
```

FW1：

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW1
[FW1]int gi 1/0/3
[FW1-GigabitEthernet1/0/3]ip address 192.168.1.1 24
[FW1-GigabitEthernet1/0/3]quit
[FW1]acl basic 2000
[FW1-acl-ipv4-basic-2000]rule 0 permit source any
[FW1-acl-ipv4-basic-2000]quit
[FW1]int gi 1/0/2
[FW1-GigabitEthernet1/0/2]des <connect to ISP>
[FW1-GigabitEthernet1/0/2]ip address 202.1.100.2 30
[FW1-GigabitEthernet1/0/2]nat outbound 2000
[FW1-GigabitEthernet1/0/2]quit
[FW1]security-zone name Trust
[FW1-security-zone-Trust]import interface GigabitEthernet 1/0/3
```

```
[FW1-security-zone-Trust]quit
[FW1]security-zone name Untrust
[FW1-security-zone-Untrust]import interface GigabitEthernet 1/0/2
[FW1-security-zone-Untrust]quit

[FW1]ip route-static 0.0.0.0 0.0.0.0 202.1.100.1
[FW1]acl basic 2001
[FW1-acl-ipv4-basic-2001]rule 0 permit source any
[FW1-acl-ipv4-basic-2001]quit
[FW1]
[FW1]zone-pair security source trust destination untrust
[FW1-zone-pair-security-Trust-Untrust]packet-filter 2001
[FW1-zone-pair-security-Trust-Untrust]quit
[FW1]
[FW1]zone-pair security source untrust destination trust
[FW1-zone-pair-security-Untrust-Trust]packet-filter 2001
[FW1-zone-pair-security-Untrust-Trust]quit
[FW1]
[FW1]zone-pair security source trust destination local
[FW1-zone-pair-security-Trust-Local]packet-filter 2001
[FW1-zone-pair-security-Trust-Local]quit
[FW1]
[FW1]zone-pair security source local destination trust
[FW1-zone-pair-security-Local-Trust]packet-filter 2001
[FW1-zone-pair-security-Local-Trust]quit
[FW1]
[FW1]zone-pair security source untrust destination local
[FW1-zone-pair-security-Untrust-Local]packet-filter 2001
[FW1-zone-pair-security-Untrust-Local]quit
[FW1]
[FW1]zone-pair security source local destination untrust
[FW1-zone-pair-security-Local-Untrust]packet-filter 2001
[FW1-zone-pair-security-Local-Untrust]quit
```

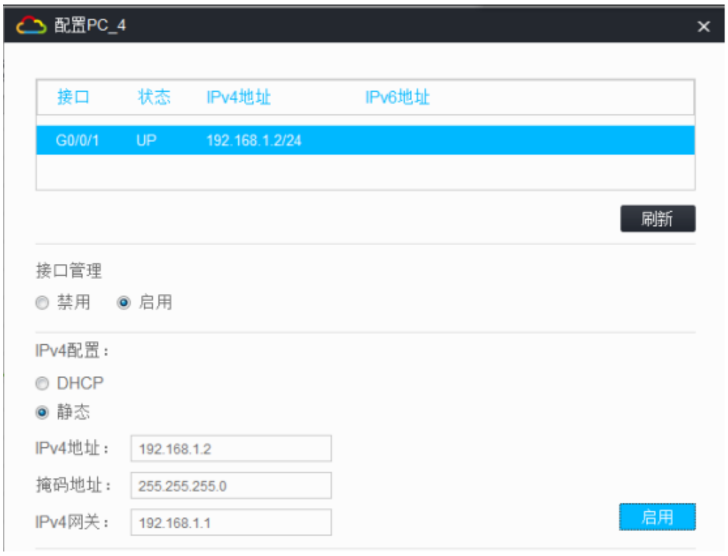
FW2：

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW2
[FW2]int gi 1/0/3
[FW2-GigabitEthernet1/0/3]ip address 172.16.1.1 24
[FW2-GigabitEthernet1/0/3]quit
[FW2]acl basic 2000
[FW2-acl-ipv4-basic-2000]rule 0 permit source any
[FW2-acl-ipv4-basic-2000]quit
[FW2]int gi 1/0/2
[FW2-GigabitEthernet1/0/2]des <connect to ISP>
[FW2-GigabitEthernet1/0/2]ip address 202.2.100.2 30
[FW2-GigabitEthernet1/0/2]nat outbound 2000
[FW2-GigabitEthernet1/0/2]quit
[FW2]ip route-static 0.0.0.0 0.0.0.0 202.2.100.1
[FW2]security-zone name Trust
[FW2-security-zone-Trust]import interface GigabitEthernet 1/0/3
[FW2-security-zone-Trust]quit
[FW2]security-zone name Untrust
[FW2-security-zone-Untrust]import interface GigabitEthernet 1/0/2
[FW2-security-zone-Untrust]quit
[FW2]acl basic 2001
[FW2-acl-ipv4-basic-2001]rule 0 permit source any
[FW2-acl-ipv4-basic-2001]quit
[FW2]
[FW2]zone-pair security source trust destination untrust
[FW2-zone-pair-security-Trust-Untrust]packet-filter 2001
[FW2-zone-pair-security-Trust-Untrust]quit
[FW2]
```

```
[FW2]zone-pair security source untrust destination trust
[FW2-zone-pair-security-Untrust-Trust]packet-filter 2001
[FW2-zone-pair-security-Untrust-Trust]quit
[FW2]
[FW2]zone-pair security source trust destination local
[FW2-zone-pair-security-Trust-Local]packet-filter 2001
[FW2-zone-pair-security-Trust-Local]quit
[FW2]
[FW2]zone-pair security source local destination trust
[FW2-zone-pair-security-Local-Trust]packet-filter 2001
[FW2-zone-pair-security-Local-Trust]quit
[FW2]
[FW2]zone-pair security source untrust destination local
[FW2-zone-pair-security-Untrust-Local]packet-filter 2001
[FW2-zone-pair-security-Untrust-Local]quit
[FW2]
[FW2]zone-pair security source local destination untrust
[FW2-zone-pair-security-Local-Untrust]packet-filter 2001
[FW2-zone-pair-security-Local-Untrust]quit
```

第一阶段测试：

所有PC都填写IP地址：



接口	状态	IPv4地址	IPv6地址
G0/0/1	UP	192.168.1.2/24	

接口管理

○ 禁用 ● 启用

IPv4配置：

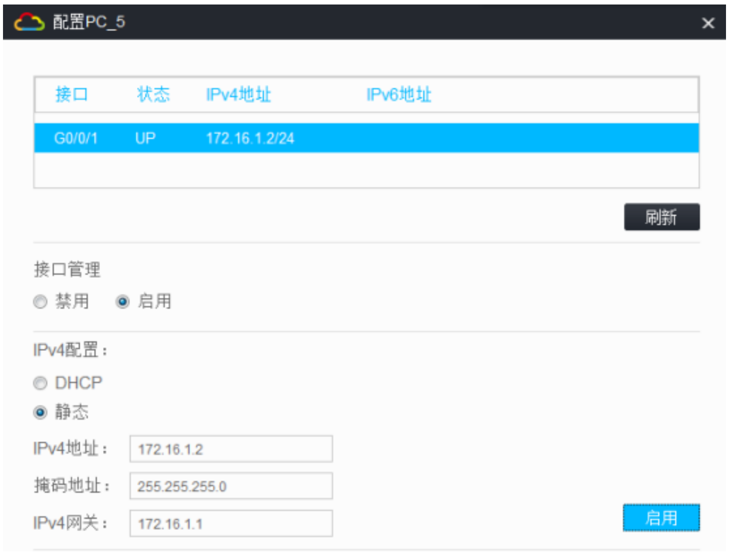
○ DHCP

● 静态

IPv4地址：192.168.1.2

掩码地址：255.255.255.0

IPv4网关：192.168.1.1



接口	状态	IPv4地址	IPv6地址
G0/0/1	UP	172.16.1.2/24	

接口管理

○ 禁用 ● 启用

IPv4配置：

○ DHCP

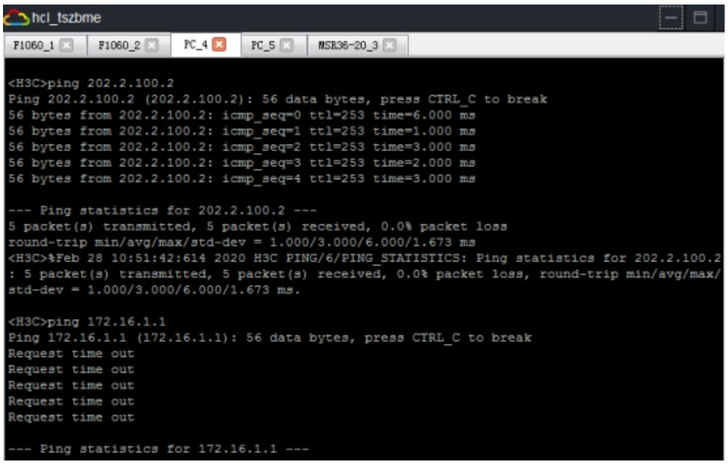
● 静态

IPv4地址：172.16.1.2

掩码地址：255.255.255.0

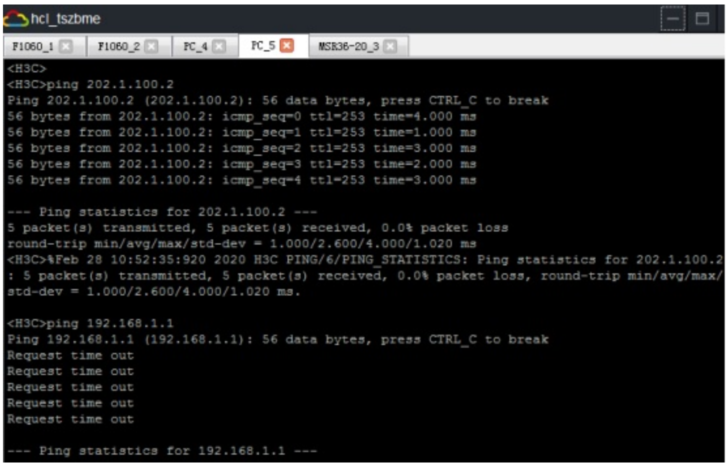
IPv4网关：172.16.1.1

内网1的终端仅能PING通内网2的外网地址，PING不通私网地址：



```
<H3C>ping 202.2.100.2
Ping 202.2.100.2 (202.2.100.2): 56 data bytes, press CTRL_C to break
56 bytes from 202.2.100.2: icmp_seq=0 ttl=253 time=6.000 ms
56 bytes from 202.2.100.2: icmp_seq=1 ttl=253 time=1.000 ms
56 bytes from 202.2.100.2: icmp_seq=2 ttl=253 time=3.000 ms
56 bytes from 202.2.100.2: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 202.2.100.2: icmp_seq=4 ttl=253 time=3.000 ms

--- Ping statistics for 202.2.100.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/3.000/6.000/1.673 ms
<H3C>%Feb 28 10:51:42:614 2020 H3C PING/6/PING_STATISTICS: Ping statistics for 202.2.100.2
: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/
std-dev = 1.000/3.000/6.000/1.673 ms.

<H3C>ping 172.16.1.1
Ping 172.16.1.1 (172.16.1.1): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 172.16.1.1 ---
```

内网2的终端仅能PING通内网1的外网地址，PING不通私网地址：



```
<H3C>
<H3C>ping 202.1.100.2
Ping 202.1.100.2 (202.1.100.2): 56 data bytes, press CTRL_C to break
56 bytes from 202.1.100.2: icmp_seq=0 ttl=253 time=4.000 ms
56 bytes from 202.1.100.2: icmp_seq=1 ttl=253 time=1.000 ms
56 bytes from 202.1.100.2: icmp_seq=2 ttl=253 time=3.000 ms
56 bytes from 202.1.100.2: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 202.1.100.2: icmp_seq=4 ttl=253 time=3.000 ms

--- Ping statistics for 202.1.100.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.600/4.000/1.020 ms
<H3C>%Feb 28 10:52:35:920 2020 H3C PING/6/PING_STATISTICS: Ping statistics for 202.1.100.2
: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/
std-dev = 1.000/2.600/4.000/1.020 ms.

<H3C>ping 192.168.1.1
Ping 192.168.1.1 (192.168.1.1): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 192.168.1.1 ---
```

第二阶段调试（GRE VPN关键配置点：）

FW1：

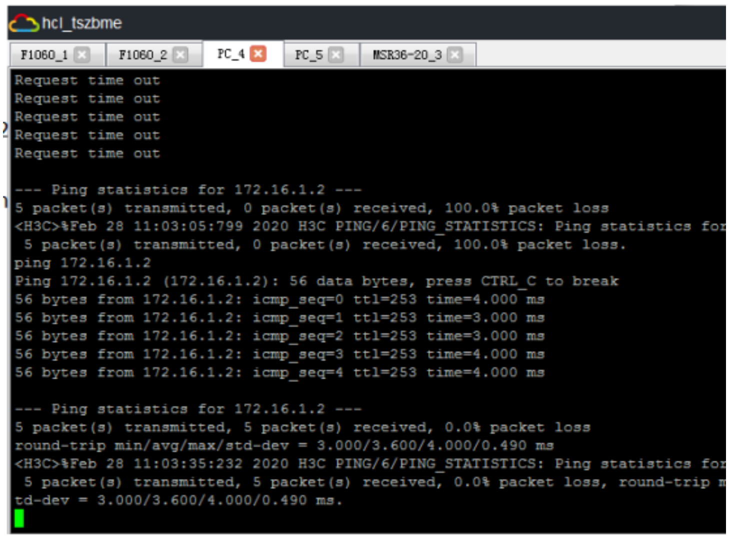
```
[FW1]int Tunnel 0 mode gre
[FW1-Tunnel0]ip address 123.0.0.1 30
[FW1-Tunnel0]source 202.1.100.2
[FW1-Tunnel0]destination 202.2.100.2
[FW1-Tunnel0]quit
[FW1]ip route-static 172.16.1.0 255.255.255.0 123.0.0.2
[FW1]security-zone name Untrust
[FW1-security-zone-Untrust]import interface Tunnel 0
[FW1-security-zone-Untrust]quit
```

FW2：

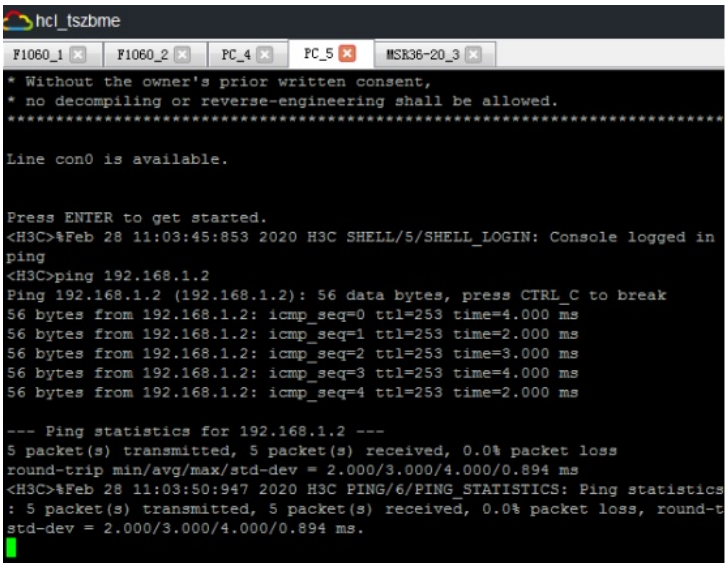
```
[FW2]int Tunnel 0 mode gre
[FW2-Tunnel0]ip address 123.0.0.2 30
[FW2-Tunnel0]source GigabitEthernet 1/0/2
[FW2-Tunnel0]description 202.1.100.2
[FW2-Tunnel0]quit
[FW2]ip route-static 192.168.1.0 255.255.255.0 123.0.0.1
[FW2]security-zone name Untrust
[FW2-security-zone-Untrust]import interface Tunnel 0
[FW2-security-zone-Untrust]quit
```

第二阶段测试：

内网1和内网2的主机可以相互PING通

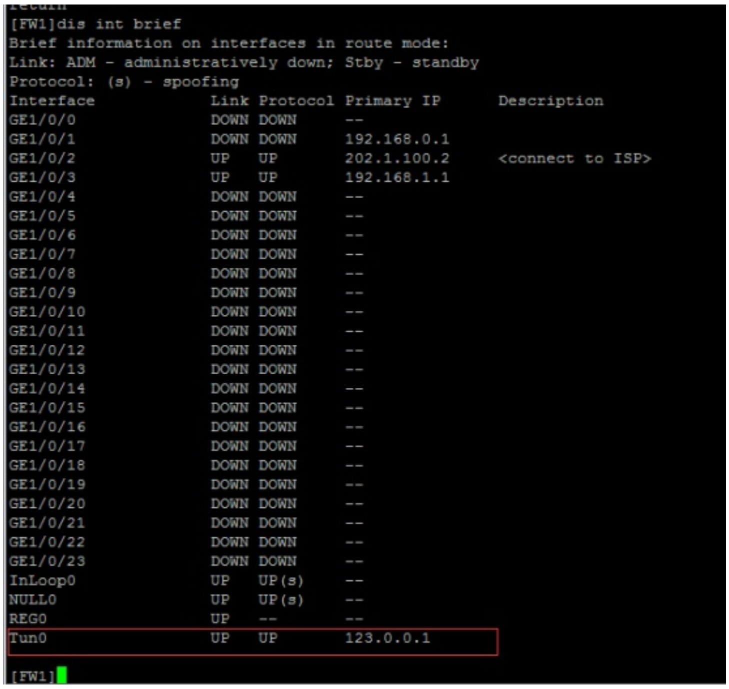


```
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 172.16.1.2 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
<H3C>%Feb 28 11:03:05:799 2020 H3C PING/6/PING_STATISTICS: Ping statistics for
 5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss.
ping 172.16.1.2
Ping 172.16.1.2 (172.16.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.1.2: icmp_seq=0 ttl=253 time=4.000 ms
56 bytes from 172.16.1.2: icmp_seq=1 ttl=253 time=3.000 ms
56 bytes from 172.16.1.2: icmp_seq=2 ttl=253 time=3.000 ms
56 bytes from 172.16.1.2: icmp_seq=3 ttl=253 time=4.000 ms
56 bytes from 172.16.1.2: icmp_seq=4 ttl=253 time=4.000 ms

--- Ping statistics for 172.16.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 3.000/3.600/4.000/0.490 ms
<H3C>%Feb 28 11:03:35:232 2020 H3C PING/6/PING_STATISTICS: Ping statistics for
 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip m
td-dev = 3.000/3.600/4.000/0.490 ms.
```

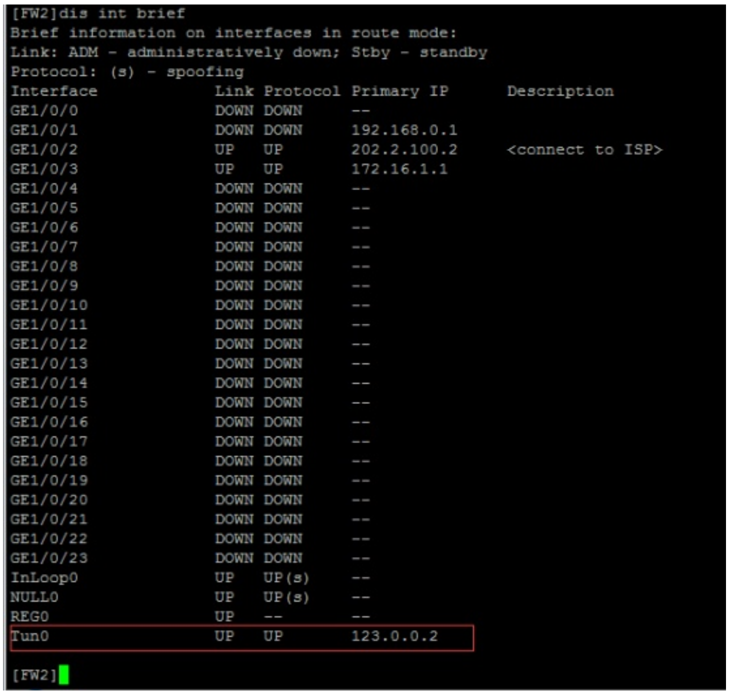


```
* Without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed.
**************************************************************************

Line con0 is available.


Press ENTER to get started.
<H3C>%Feb 28 11:03:45:853 2020 H3C SHELL/5/SHELL_LOGIN: Console logged in
ping
<H3C>ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=253 time=4.000 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=253 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=253 time=3.000 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=253 time=4.000 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=253 time=2.000 ms

--- Ping statistics for 192.168.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.000/3.000/4.000/0.894 ms
<H3C>%Feb 28 11:03:50:947 2020 H3C PING/6/PING_STATISTICS: Ping statistics
: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-t
std-dev = 2.000/3.000/4.000/0.894 ms.
```

查看FW1和FW2的隧道状态均为UP：

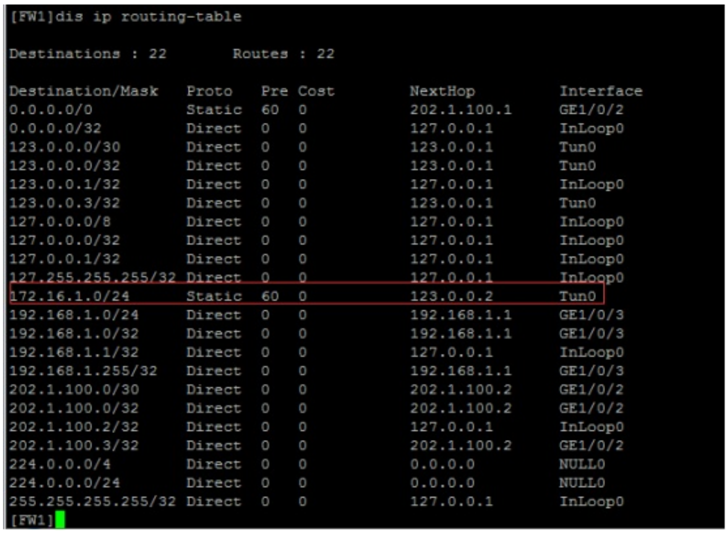


```
return
[FW1]dis int brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
GE1/0/0              DOWN DOWN     --
GE1/0/1              DOWN DOWN     192.168.0.1
GE1/0/2              UP   UP       202.1.100.2     <connect to ISP>
GE1/0/3              UP   UP       192.168.1.1
GE1/0/4              DOWN DOWN     --
GE1/0/5              DOWN DOWN     --
GE1/0/6              DOWN DOWN     --
GE1/0/7              DOWN DOWN     --
GE1/0/8              DOWN DOWN     --
GE1/0/9              DOWN DOWN     --
GE1/0/10             DOWN DOWN     --
GE1/0/11             DOWN DOWN     --
GE1/0/12             DOWN DOWN     --
GE1/0/13             DOWN DOWN     --
GE1/0/14             DOWN DOWN     --
GE1/0/15             DOWN DOWN     --
GE1/0/16             DOWN DOWN     --
GE1/0/17             DOWN DOWN     --
GE1/0/18             DOWN DOWN     --
GE1/0/19             DOWN DOWN     --
GE1/0/20             DOWN DOWN     --
GE1/0/21             DOWN DOWN     --
GE1/0/22             DOWN DOWN     --
GE1/0/23             DOWN DOWN     --
InLoop0              UP   UP(s)    --
NULL0                UP   UP(s)    --
REG0                 UP   --       --
Tun0                 UP   UP       123.0.0.1

[FW1]
```

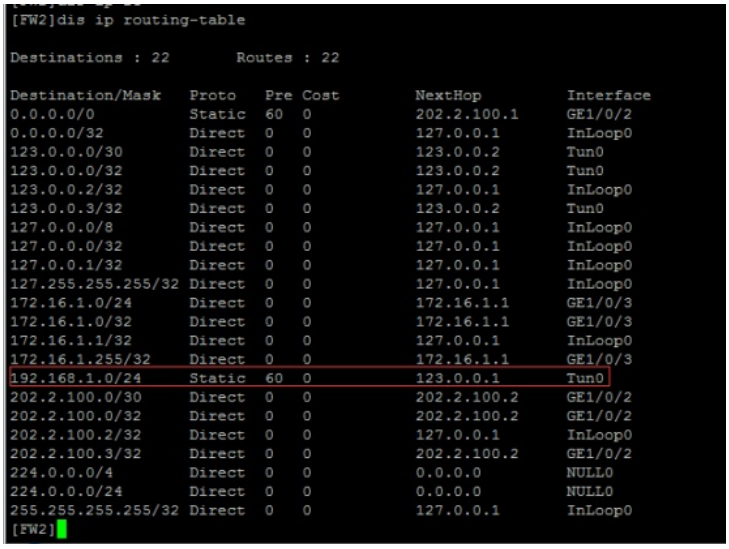


```
[FW2]dis int brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
GE1/0/0              DOWN DOWN     --
GE1/0/1              DOWN DOWN     192.168.0.1
GE1/0/2              UP   UP       202.2.100.2     <connect to ISP>
GE1/0/3              UP   UP       172.16.1.1
GE1/0/4              DOWN DOWN     --
GE1/0/5              DOWN DOWN     --
GE1/0/6              DOWN DOWN     --
GE1/0/7              DOWN DOWN     --
GE1/0/8              DOWN DOWN     --
GE1/0/9              DOWN DOWN     --
GE1/0/10             DOWN DOWN     --
GE1/0/11             DOWN DOWN     --
GE1/0/12             DOWN DOWN     --
GE1/0/13             DOWN DOWN     --
GE1/0/14             DOWN DOWN     --
GE1/0/15             DOWN DOWN     --
GE1/0/16             DOWN DOWN     --
GE1/0/17             DOWN DOWN     --
GE1/0/18             DOWN DOWN     --
GE1/0/19             DOWN DOWN     --
GE1/0/20             DOWN DOWN     --
GE1/0/21             DOWN DOWN     --
GE1/0/22             DOWN DOWN     --
GE1/0/23             DOWN DOWN     --
InLoop0              UP   UP(s)    --
NULL0                UP   UP(s)    --
REG0                 UP   --       --
Tun0                 UP   UP       123.0.0.2

[FW2]
```

查看FW1和FW2的路由表，均可看到隧道的路由：



```
[FW1]dis ip routing-table

Destinations : 22       Routes : 22

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
0.0.0.0/0           Static  60   0            202.1.100.1     GE1/0/2
0.0.0.0/32          Direct  0    0            127.0.0.1       InLoop0
123.0.0.0/30        Direct  0    0            123.0.0.1       Tun0
123.0.0.0/32        Direct  0    0            123.0.0.1       Tun0
123.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
123.0.0.3/32        Direct  0    0            123.0.0.1       Tun0
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0            127.0.0.1       InLoop0
172.16.1.0/24       Static  60   0            123.0.0.2       Tun0
192.168.1.0/24      Direct  0    0            192.168.1.1     GE1/0/3
192.168.1.0/32      Direct  0    0            192.168.1.1     GE1/0/3
192.168.1.1/32      Direct  0    0            127.0.0.1       InLoop0
192.168.1.255/32    Direct  0    0            192.168.1.1     GE1/0/3
202.1.100.0/30      Direct  0    0            202.1.100.2     GE1/0/2
202.1.100.0/32      Direct  0    0            202.1.100.2     GE1/0/2
202.1.100.2/32      Direct  0    0            127.0.0.1       InLoop0
202.1.100.3/32      Direct  0    0            202.1.100.2     GE1/0/2
224.0.0.0/4         Direct  0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct  0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct  0    0            127.0.0.1       InLoop0
[FW1]
```



```
[FW2]dis ip routing-table

Destinations : 22       Routes : 22

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
0.0.0.0/0           Static  60   0            202.2.100.1     GE1/0/2
0.0.0.0/32          Direct  0    0            127.0.0.1       InLoop0
123.0.0.0/30        Direct  0    0            123.0.0.2       Tun0
123.0.0.0/32        Direct  0    0            123.0.0.2       Tun0
123.0.0.2/32        Direct  0    0            127.0.0.1       InLoop0
123.0.0.3/32        Direct  0    0            123.0.0.2       Tun0
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0            127.0.0.1       InLoop0
172.16.1.0/24       Direct  0    0            172.16.1.1      GE1/0/3
172.16.1.0/32       Direct  0    0            172.16.1.1      GE1/0/3
172.16.1.1/32       Direct  0    0            127.0.0.1       InLoop0
172.16.1.255/32     Direct  0    0            172.16.1.1      GE1/0/3
192.168.1.0/24      Static  60   0            123.0.0.1       Tun0
202.2.100.0/30      Direct  0    0            202.2.100.2     GE1/0/2
202.2.100.0/32      Direct  0    0            202.2.100.2     GE1/0/2
202.2.100.2/32      Direct  0    0            127.0.0.1       InLoop0
202.2.100.3/32      Direct  0    0            202.2.100.2     GE1/0/2
224.0.0.0/4         Direct  0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct  0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct  0    0            127.0.0.1       InLoop0
[FW2]
```

至此，F1060 GRE VPN典型组网配置案例已完成！