MSR 系列路由器 GRE over IPsec + OSPF 穿越 NAT 多分支互通功能的配置举例

目 录

1 简介

本文档介绍 MSR 系列路由器 GRE over IPsec + OSPF 穿越 NAT 多分支互通功能的典型配置案例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 GRE、IPsec 和 OSPF 特性。

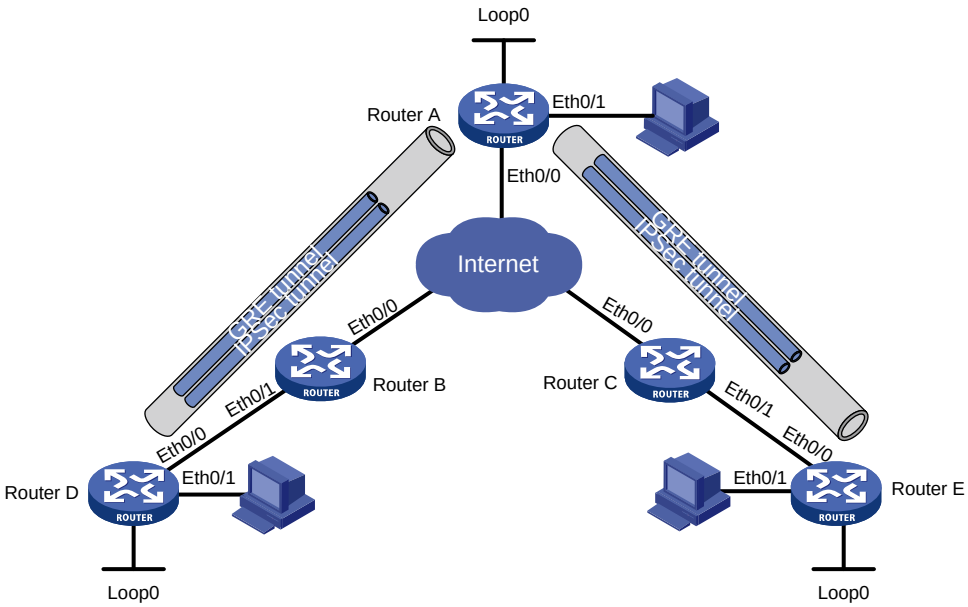
3 配置举例

3.1 组网需求

如 图 1 所示，Router A为某机构总部，Router D和Router E为分支，Router B和Router C为两个分支出口的NAT设备。要求：

- 总部和分支内网之间通过 Loopback 口建立 GRE 隧道实现互通。
- 总部采用安全模板方式建立 IPsec 隧道保护 GRE 隧道的数据流。
- 在 GRE 隧道上运行 OSPF，使各内部路由互通，分支之间的流量通过总部转发。

图1 MSR 系列路由器 GRE Over IPSec + OSPF 穿越 NAT 多分支互通功能的配置组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	Eth0/0	1.0.0.60/24	Router D	Eth0/0	10.0.1.2/24
	Eth0/1	172.1.1.1/24		Eth0/1	192.168.11.1
	Loop0	172.0.0.1/32		Loop0	192.168.1.1/32

Router B	Eth0/0	1.0.0.1/24	Router E	Eth0/0	10.0.2.2/24
	Eth0/1	10.0.1.1/24		Eth0/1	192.168.12.1/24
Router C	Eth0/0	1.0.0.2/24		Loop0	192.168.2.1/32
	Eth0/1	10.0.2.1/24			

3.2 配置思路

为了穿越分支出口的 NAT 设备，总部和分支之间需要配置成野蛮模式并启用 NAT 穿越。

3.3 使用版本

本举例是在 Release 2317 版本上进行配置和验证的。

3.4 配置注意事项

- 建立 GRE 隧道的地址必须是内网地址。
- 不能将建立 GRE 隧道连接的 Loopback 接口加入到 OSPF，否则连接会失效。

3.5 配置步骤

3.5.1 Router A的配置

配置接口 Ethernet0/0 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface ethernet 0/0
[RouterA-Ethernet0/0] ip address 1.0.0.60 255.255.255.0
[RouterA-Ethernet0/0] quit
```

配置接口 Ethernet0/1 的 IP 地址。

```
[RouterA] interface ethernet 0/1
[RouterA-Ethernet0/1] ip address 172.1.1.1 255.255.255.0
[RouterA-Ethernet0/1] quit
```

配置用于 GRE 连接和 OSPF Router ID 的 Loopback 接口地址。

```
[RouterA] interface loopback 0
[RouterA-LoopBack0] ip address 172.0.0.1 255.255.255.0
[RouterA-LoopBack0] quit
```

配置到 NAT 设备的静态路由，目的地址为 NAT 转换后的地址。

```
[RouterA] ip route-static 11.0.0.0 255.0.0.0 1.0.0.1
[RouterA] ip route-static 12.0.0.0 255.0.0.0 1.0.0.2
```

配置到分支环回口的静态路由。

```
[RouterA] ip route-static 192.168.1.1 255.255.255.255 1.0.0.1
[RouterA] ip route-static 192.168.2.1 255.255.255.255 1.0.0.2
```

配置到 branch1 的 GRE 隧道。

```
[RouterA] interface tunnel 0
[RouterA-Tunnel0] ip address 192.168.0.1 255.255.255.252
[RouterA-Tunnel0] source LoopBack 0
```

```
[RouterA-Tunnel0] destination 192.168.1.1
[RouterA-Tunnel0] quit
```
配置到 branch2 的 GRE 隧道。
```
[RouterA] interface tunnel 1
[RouterA-Tunnel1] ip address 192.168.0.5 255.255.255.252
[RouterA-Tunnel1] source loopback0
[RouterA-Tunnel1] destination 192.168.2.1
[RouterA-Tunnel1] quit
```
配置 OSPF 路由协议。
```
[RouterA] router id 172.0.0.1
[RouterA] ospf 1
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.3
[RouterA-ospf-1-area-0.0.0.0] network 192.168.0.4 0.0.0.3
[RouterA-ospf-1-area-0.0.0.0] quit
```
配置本端安全网关的名字为 center。
```
[RouterA] ike local-name center
```
配置 IKE 对等体 branch1。
```
[RouterA] ike peer branch1
[RouterA-ike-peer-branch1] exchange-mode aggressive
[RouterA-ike-peer-branch1] pre-shared-key 123
[RouterA-ike-peer-branch1] id-type name
[RouterA-ike-peer-branch1] remote-name branch1
[RouterA-ike-peer-branch1] nat traversal
[RouterA-ike-peer-branch1] quit
```
配置 IKE 对等体 branch2。
```
[RouterA] ike peer branch2
[RouterA-ike-peer-branch2] exchange-mode aggressive
[RouterA-ike-peer-branch2] pre-shared-key 123
[RouterA-ike-peer-branch2] id-type name
[RouterA-ike-peer-branch2] remote-name branch2
[RouterA-ike-peer-branch2] nat traversal
[RouterA-ike-peer-branch2] quit
```
采用安全提议的缺省配置。
```
[RouterA] ipsec proposal def
```
配置 ESP 协议采用 md5 认证算法。
```
[RouterA-ipsec-transform-set-def] esp authentication-algorithm md5
[RouterA-ipsec-transform-set-def] quit
```
创建 IPsec 安全策略模板 branch1。
```
[RouterA] ipsec policy-template branch1 1
[RouterA-ipsec-policy-template-branch1-1] ike-peer branch1
[RouterA-ipsec-policy-template-branch1-1] proposal def
[RouterA-ipsec-policy-template-branch1-1] quit
```
引用 IPsec 安全策略模板创建一条 IPsec 安全策略。

```
[RouterA] ipsec policy branch 1 isakmp template branch1
```
创建 IPsec 安全策略模板 branch2。
```
[RouterA] ipsec policy-template branch2 1
[RouterA-ipsec-policy-template-branch2-1] ike-peer branch2
[RouterA-ipsec-policy-template-branch2-1] proposal def
[RouterA-ipsec-policy-template-branch2-1] quit
```
引用 IPsec 安全策略模板创建一条 IPsec 安全策略。
```
[RouterA] ipsec policy branch 2 isakmp template branch2
```
在接口 Ethernet0/0 上应用安全策略。
```
[RouterA] interface ethernet 0/0
[RouterA-Ethernet0/0] ipsec policy branch
[RouterA-Ethernet0/0] quit
```

3.5.2 Router B的配置

配置接口 Ethernet0/0 的 IP 地址。
```
<RouterB> system-view
[RouterB] interface ethernet 0/0
[RouterB-Ethernet0/0] ip address 1.0.0.1 255.255.255.0
[RouterB-Ethernet0/0] quit
```
配置接口 Ethernet0/1 的 IP 地址。
```
[RouterB] interface ethernet 0/1
[RouterB-Ethernet0/1] ip address 10.0.1.1 255.255.255.0
[RouterB-Ethernet0/1] quit
```
创建 NAT 转换地址池。
```
[RouterB] nat address-group 0 11.0.0.1 11.0.0.10
```
创建 ACL2000，定义需要 NAT 转换的数据流。
```
[RouterB] acl number 2000
[RouterB-acl-basic-2000] rule 0 permit source 10.0.1.0 0.0.0.255
[RouterB-acl-basic-2000] quit
```
在接口下配置访问控制列表和地址池关联。
```
[RouterB] interface ethernet 0/0
[RouterB-Ethernet0/0] nat outbound 2000 address-group 0
[RouterB-Ethernet0/0] quit
```

3.5.3 Router C的配置

配置接口 Ethernet0/0 的 IP 地址。
```
<RouterC> system-view
[RouterC] interface ethernet 0/0
[RouterC-Ethernet0/0] ip address 1.0.0.2 255.255.255.0
[RouterC-Ethernet0/0] quit
```
配置接口 Ethernet0/1 的 IP 地址。
```
[RouterC] interface ethernet 0/1
[RouterC-Ethernet0/1] ip address 10.0.2.1 255.255.255.0
```

```
[RouterC-Ethernet0/1] quit
```
创建 NAT 转换地址池。
```
[RouterC] nat address-group 0 12.0.0.1 12.0.0.10
```
创建 ACL2000,定义需要 NAT 转换的数据流。
```
[RouterC] acl number 2000
[RouterC-acl-basic-2000] rule 0 permit source 10.0.2.0 0.0.0.255
[RouterC-acl-basic-2000] quit
```
在接口下配置访问控制列表和地址池关联。
```
[RouterC] interface ethernet 0/0
[RouterC-Ethernet0/0] nat outbound 2000 address-group 0
[RouterC-Ethernet0/0] quit
```
3.5.4 Router D的配置

配置接口 Ethernet0/0 的 IP 地址。
```
<RouterD> system-view
[RouterD] interface ethernet 0/0
[RouterD-Ethernet0/0] ip address 10.0.1.2 255.255.255.0
[RouterD-Ethernet0/0] quit
```
配置接口 Ethernet0/1 的 IP 地址。
```
[RouterD] interface ethernet 0/1
[RouterD-Ethernet0/1] ip address 192.168.11.1 255.255.255.0
[RouterD-Ethernet0/1] quit
```
配置用于 GRE 连接和 OSPF Router ID 的 Loopback 接口地址。
```
[RouterD] interface loopback 0
[RouterD-LoopBack0] ip address 192.168.1.1 255.255.255.255
[RouterD-LoopBack0] quit
```
配置访问外网的默认路由。
```
[RouterD] ip route-static 0.0.0.0 0.0.0.0 10.0.1.1
```
配置到 center 的 GRE 隧道。
```
[RouterD] interface tunnel 0
[RouterD-Tunnel0] ip address 192.168.0.2 255.255.255.252
[RouterD-Tunnel0] source Loopback0
[RouterD-Tunnel0] destination 172.0.0.1
[RouterD-Tunnel0] quit
```
配置 OSPF 路由协议。
```
[RouterD] router id 192.168.1.1
[RouterD] ospf 1
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 192.168.11.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.3
[RouterD-ospf-1-area-0.0.0.0] quit
```
配置本端安全网关的名字为 branch1。
```
[RouterD] ike local-name branch1
```
创建 ACL3000,定义需要 IPsec 保护的数据流。

```
[RouterD] acl number 3000
[RouterD-acl-adv-3000] rule 0 permit gre source 192.168.1.1 0 destination 172.0.0
.1 0
[RouterD-acl-adv-3000] quit
```
配置 IKE 对等体 center。
```
[RouterD] ike peer center
[RouterD-ike-peer-center] exchange-mode aggressive
[RouterD-ike-peer-center] pre-shared-key 123
[RouterD-ike-peer-center] id-type name
[RouterD-ike-peer-center] remote-name center
[RouterD-ike-peer-center] remote-address 1.0.0.60
[RouterD-ike-peer-center] nat traversal
[RouterD-ike-peer-center] quit
```
采用安全提议的缺省配置。
```
[RouterD] ipsec proposal def
```
配置 ESP 协议采用 md5 认证算法。
```
[RouterD-ipsec-transform-set-def] esp authentication-algorithm md5
[RouterD-ipsec-transform-set-def] quit
```
创建 IPsec 安全策略 center，其协商方式为 isakmp。
```
[RouterD] ipsec policy center 1 isakmp
[RouterD-ipsec-policy-isakmp-center-1] security acl 3000
[RouterD-ipsec-policy-isakmp-center-1] ike-peer center
[RouterD-ipsec-policy-isakmp-center-1] proposal def
[RouterD-ipsec-policy-isakmp-center-1] quit
```
在接口 Ethernet0/0 上应用安全策略。
```
[RouterD] interface ethernet 0/0
[RouterD-Ethernet0/0] ipsec policy center
[RouterD-Ethernet0/0] quit
```

3.5.5 Router E的配置

配置接口 Ethernet0/0 的 IP 地址。
```
<RouterE> system-view
[RouterE] interface ethernet 0/0
[RouterE-Ethernet0/0] ip address 10.0.2.2 255.255.255.0
[RouterE-Ethernet0/0] quit
```
配置接口 Ethernet0/1 的 IP 地址。
```
[RouterE] interface ethernet 0/1
[RouterE-Ethernet0/1] ip address 192.168.12.1 255.255.255.0
[RouterE-Ethernet0/1] quit
```
配置用于 GRE 连接和 OSPF Router ID 的 Loopback 接口地址。
```
[RouterE] interface loopback 0
[RouterE-LoopBack0] ip address 192.168.2.1 255.255.255.255
[RouterE-LoopBack0] quit
```
配置访问外网的默认路由。

```
[RouterE] ip route-static 0.0.0.0 0.0.0.0 10.0.2.1
```
配置到 center 的 GRE 隧道。
```
[RouterE] interface tunnel 0
[RouterE-Tunnel0] ip address 192.168.0.6 255.255.255.252
[RouterE-Tunnel0] source loopback0
[RouterE-Tunnel0] destination 172.0.0.1
[RouterE-Tunnel0] quit
```
配置 OSPF 路由协议。
```
[RouterE] router id 192.168.2.1
[RouterE] ospf 1
[RouterE-ospf-1] area 0
[RouterE-ospf-1-area-0.0.0.0] network 192.168.0.4 0.0.0.3
[RouterE-ospf-1-area-0.0.0.0] network 192.168.12.0 0.0.0.255
[RouterE-ospf-1-area-0.0.0.0] quit
```
配置本端安全网关的名字为 branch2。
```
[RouterE] ike local-name branch2
```
创建 ACL3000,定义需要 IPsec 保护的数据流。
```
[RouterE] acl number 3000
[RouterE-acl-adv-3000] rule 0 permit gre source 192.168.2.1 0 destination 172.0.
0.1 0
[RouterE-acl-adv-3000] quit
```
配置 IKE 对等体 center。
```
[RouterE] ike peer center
[RouterE-ike-peer-center] exchange-mode aggressive
[RouterE-ike-peer-center] pre-shared-key 123
[RouterE-ike-peer-center] id-type name
[RouterE-ike-peer-center] remote-name center
[RouterE-ike-peer-center] remote-address 1.0.0.60
[RouterE-ike-peer-center] nat traversal
[RouterE-ike-peer-center] quit
```
采用安全提议的缺省配置。
```
[RouterE] ipsec proposal def
```
配置 ESP 协议采用 md5 认证算法。
```
[RouterE-ipsec-transform-set-def] esp authentication-algorithm md5
[RouterE-ipsec-transform-set-def] quit
```
创建 IPsec 安全策略 center，其协商方式为 isakmp。
```
[RouterE] ipsec policy center 1 isakmp
[RouterE-ipsec-policy-isakmp-center-1] security acl 3000
[RouterE-ipsec-policy-isakmp-center-1] ike-peer center
[RouterE-ipsec-policy-isakmp-center-1] proposal def
[RouterE-ipsec-policy-isakmp-center-1] quit
```
在接口 Ethernet0/0 上应用安全策略。
```
[RouterE] interface ethernet 0/0
[RouterE-Ethernet0/0] ipsec policy center
[RouterE-Ethernet0/0] quit
```

3.6 验证配置

完成以上配置后，总部和分支间的内网之间可以互通，且数据进行了 IPsec 加密。此处以 Router D 为例进行验证，Router A 和 Router E 验证方法相同。

通过以下显示信息看到，Router D 和 Router A 的内网间可以通信。

```
<RouterD> ping -a 192.168.11.1 172.1.1.1
  PING 172.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 172.1.1.1: bytes=56 Sequence=0 ttl=255 time=3 ms
    Reply from 172.1.1.1: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 172.1.1.1: bytes=56 Sequence=2 ttl=255 time=3 ms
    Reply from 172.1.1.1: bytes=56 Sequence=3 ttl=255 time=3 ms
    Reply from 172.1.1.1: bytes=56 Sequence=4 ttl=255 time=3 ms

  --- 172.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 2/2/3 ms
```

通过以下显示信息看到，Router D 和 Router E 的内网间可以通信。

```
<RouterD> ping -a 192.168.11.1 192.168.12.1
  PING 192.168.12.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.12.1: bytes=56 Sequence=0 ttl=254 time=5 ms
    Reply from 192.168.12.1: bytes=56 Sequence=1 ttl=254 time=4 ms
    Reply from 192.168.12.1: bytes=56 Sequence=2 ttl=254 time=4 ms
    Reply from 192.168.12.1: bytes=56 Sequence=3 ttl=254 time=5 ms
    Reply from 192.168.12.1: bytes=56 Sequence=4 ttl=254 time=4 ms

  --- 192.168.12.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 4/4/5 ms
```

可以通过如下显示信息看到，IKE 协商成功，生成了两个阶段的 SA。

```
<RouterD> display ike sa
    total phase-1 SAs:  1
    connection-id  peer                    flag        phase   doi
  ----------------------------------------------------------------
     1             1.0.0.60                RD|ST       1       IPSEC
     2             1.0.0.60                RD|ST       2       IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT RK—REKEY
```

可以通过如下显示信息查看协商生成的 IPsec SA。

```
<RouterD> display ipsec sa
==============================
Interface: Ethernet0/0
```

```
    path MTU: 1500
================================

  -----------------------------
  IPsec policy name: "center"
  sequence number: 1
  acl version: ACL4
  mode: isakmp
  -----------------------------
    PFS: N, DH group: none
    tunnel:
        local  address: 10.0.1.2
        remote address: 1.0.0.60
    flow:
        sour addr: 192.168.1.1/255.255.255.255  port: 0  protocol: GRE
        dest addr: 172.0.0.1/255.255.255.255  port: 0  protocol: GRE

    [inbound ESP SAs]
      spi: 0x63A97145(1672048965)
      transform: ESP-ENCRYPT-NULL ESP-AUTH-MD5
      in use setting: Tunnel
      connection id: 1
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843187/2747
      anti-replay detection: Enabled
        anti-replay window size(counter based): 32
      udp encapsulation used for nat traversal: Y

    [outbound ESP SAs]
      spi: 0x678E301F(1737371679)
      transform: ESP-ENCRYPT-NULL ESP-AUTH-MD5
      in use setting: Tunnel
      connection id: 2
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843190/2747
      anti-replay detection: Enable
        anti-replay window size(counter based): 32
      udp encapsulation used for nat traversal: Y
```

通过 Router D 的 Tunnel 接口状态，可以看到 GRE 隧道的已建立。

```
<RouterD> display interface tunnel0
Tunnel0 current state: UP
Line protocol current state: UP
Description: Tunnel0 Interface
The Maximum Transmit Unit is 1476
Internet Address is 192.168.0.2/30 Primary
Encapsulation is TUNNEL, service-loopback-group ID not set.
Tunnel source 192.168.1.1 (LoopBack0), destination 172.0.0.1
Tunnel bandwidth 64 (kbps)
```

```
Tunnel keepalive disabled
Tunnel protocol/transport GRE/IP
    GRE key disabled
    Checksumming of GRE packets disabled
Output queue : (Urgent queuing : Size/Length/Discards)  0/100/0
Output queue : (Protocol queuing : Size/Length/Discards)  0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
 Last clearing of counters:  Never
    Last 300 seconds input:  12 bytes/sec, 0 packets/sec
    Last 300 seconds output:  11 bytes/sec, 0 packets/sec
    568 packets input,  43463 bytes
    0 input error
    476 packets output,  32896 bytes
    0 output error
```

查看 Router D 的 OSPF 路由表信息。

```
<RouterD> display ospf routing

          OSPF Process 1 with Router ID 192.168.1.1
                  Routing Tables

 Routing for Network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 192.168.11.0/24    1        Stub    192.168.11.1    192.168.1.1     0.0.0.0
 192.168.12.0/24    3125     Stub    192.168.0.1     192.168.2.1     0.0.0.0
 192.168.0.0/30     1562     Stub    192.168.0.2     192.168.1.1     0.0.0.0
 192.168.0.4/30     3124     Stub    192.168.0.1     172.0.0.1       0.0.0.0
 172.1.1.0/24       1563     Stub    192.168.0.1     172.0.0.1       0.0.0.0

 Total Nets: 5
 Intra Area: 5  Inter Area: 0  ASE: 0  NSSA: 0
```

3.7 配置文件

- Router A：

```
#
 ike local-name center
#
router id 172.0.0.1
#
ike peer branch1
 exchange-mode aggressive
 pre-shared-key cipher $c$3$ZXoEjc/u9yOHbYf3rqsrlfng4uU9zA==
 id-type name
 remote-name branch1
 nat traversal
#
ike peer branch2
 exchange-mode aggressive
```

```
 pre-shared-key cipher $c$3$/UggNLz11JIoLL6989MDKbJA8UG2pA==
 id-type name
 remote-name branch2
 nat traversal
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy-template branch1 1
 ike-peer branch1
 transform-set def
#
ipsec policy-template branch2 1
 ike-peer branch2
 transform-set def
#
ipsec policy branch 1 isakmp template branch1
#
ipsec policy branch 2 isakmp template branch2
#
interface Ethernet0/1
 port link-mode route
 ip address 172.1.1.1 255.255.255.0
#
interface Ethernet0/0
 port link-mode route
 ip address 1.0.0.60 255.255.255.0
 ipsec policy branch
#
interface LoopBack0
 ip address 172.0.0.1 255.255.255.255
#
interface Tunnel0
 ip address 192.168.0.1 255.255.255.252
 source LoopBack0
 destination 192.168.1.1
#
interface Tunnel1
 ip address 192.168.0.5 255.255.255.252
 source LoopBack0
 destination 192.168.2.1
#
ospf 1
 area 0.0.0.0
  network 172.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.3
```

```
  network 192.168.0.4 0.0.0.3
#
 ip route-static 11.0.0.0 255.0.0.0 1.0.0.1
 ip route-static 12.0.0.0 255.0.0.0 1.0.0.2
 ip route-static 192.168.1.1 255.255.255.255 1.0.0.1
 ip route-static 192.168.2.1 255.255.255.255 1.0.0.2
#
```

- Router B：

```
#
 nat address-group 0 11.0.0.1 11.0.0.10
#
acl number 2000
 rule 0 permit source 10.0.1.0 0.0.0.255
#
interface Ethernet0/1
 port link-mode route
 ip address 10.0.1.1 255.255.255.0
#
interface Ethernet0/0
 port link-mode route
 nat outbound 2000 address-group 0
 ip address 1.0.0.1 255.255.255.0
#
```

- Router C：

```
#
 nat address-group 0 12.0.0.1 12.0.0.10
#
acl number 2000
 rule 0 permit source 10.0.2.0 0.0.0.255
#
interface Ethernet0/0
 port link-mode route
 nat outbound 2000 address-group 0
 ip address 1.0.0.2 255.255.255.0
#
interface Ethernet0/1
 port link-mode route
 ip address 10.0.2.1 255.255.255.0
#
```

- Router D：

```
#
 ike local-name branch1
#
router id 192.168.1.1
#
acl number 3000
 rule 0 permit gre source 192.168.1.1 0 destination 172.0.0.1 0
```

```
#
#
ike peer center
 exchange-mode aggressive
 pre-shared-key cipher $c$3$TzhHV0sgzcqiNJ4Kk+zLgsXR7wrGGA==
 id-type name
 remote-name center
 remote-address 1.0.0.60
 nat traversal
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy center 1 isakmp
 security acl 3000
 ike-peer center
 transform-set def
#
interface LoopBack0
 ip address 192.168.1.1 255.255.255.255
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 192.168.11.1 255.255.255.0
#
interface Ethernet0/0
 port link-mode route
 ip address 10.0.1.2 255.255.255.0
 ipsec policy center
#
interface Tunnel0
 ip address 192.168.0.2 255.255.255.252
 source LoopBack0
 destination 172.0.0.1
#
ospf 1
 area 0.0.0.0
  network 192.168.11.0 0.0.0.255
  network 192.168.0.0 0.0.0.3
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.1.1
#
```

- Router E：

```
#
 ike local-name branch2
#
```

```
router id 192.168.2.1
#
acl number 3000
 rule 0 permit gre source 192.168.2.1 0 destination 172.0.0.1 0
#
ike peer center
 exchange-mode aggressive
 pre-shared-key cipher $c$3$49IxXQ7E9AU4Yam2pysj2RUqCNQhgw==
 id-type name
 remote-name center
 remote-address 1.0.0.60
 nat traversal
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy center 1 isakmp
 security acl 3000
 ike-peer center
 transform-set def
#
interface LoopBack0
 ip address 192.168.2.1 255.255.255.255
#
interface GigabitEthernet0/1
 ip address 192.168.12.1 255.255.255.0
#
interface Ethernet0/0
 ip address 10.0.2.2 255.255.255.0
 ipsec policy center
#
interface Tunnel0
 ip address 192.168.0.6 255.255.255.252
 source LoopBack0
 destination 172.0.0.1
#
ospf 1
 area 0.0.0.0
  network 192.168.0.4 0.0.0.3
  network 192.168.12.0 0.0.0.255
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.2.1
#
```

4 相关资料

- H3C MSR 系列路由器 命令参考(V5)-R2311
- H3C MSR 系列路由器 配置指导(V5)-R2311