MSR 系列路由器 IPsec over GRE + OSPF 功能的配置举例

目 录

1 简介

本文档介绍 MSR 路由器 IPsec over GRE + OSPF 功能的典型配置举例。

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 IPsec、GRE 和 OSPF 特性。

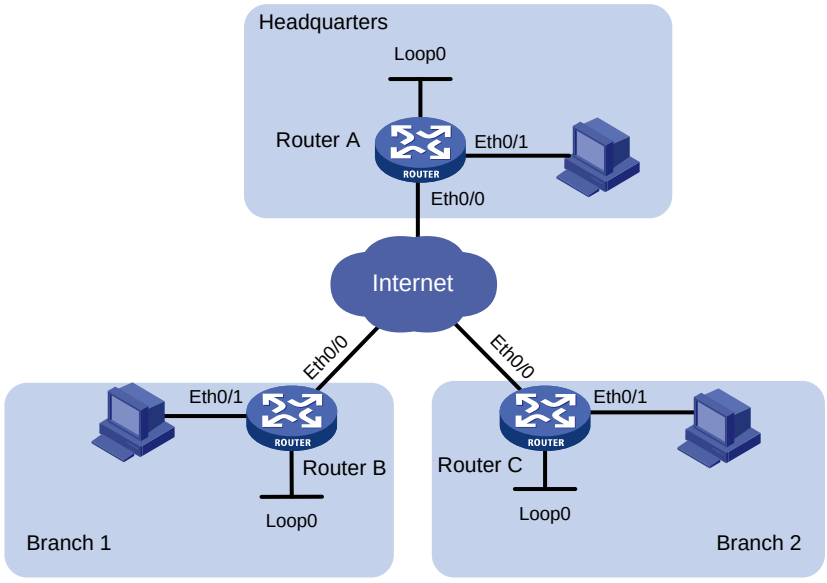
3 配置举例

3.1 组网需求

如 图 1 所示，Router A为某机构总部网关，Router B和Router C为分支网关，要求：

- 总部和分支之间建立 GRE 隧道。
- 总部和分支之间实现内网的互通。
- 运用 IPsec 技术对总部和分支内网之间指定的流量进行加密。

图1 MSR 路由器 IPsec over GRE + OSPF 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	1.0.0.254/24	Router C	Eth0/0	1.0.0.2/24
	Eth0/1	10.0.0.1/24		Eth0/1	192.168.2.1
	Loop0	192.168.255.255/32		Loop0	192.168.255.2/32
Router B	Eth0/0	1.0.0.1/24			
	Eth0/1	192.168.1.1/24			
	Loop0	192.168.255.1/32			

3.2 配置思路

- 将 GRE 隧道与 OSPF 结合使用，可以通过 GRE 来传递 OSPF 路由，从而使企业私网之间可以互通。
- 将 IPsec 与 GRE 结合使用，可以对通过 GRE 隧道的路由即企业私网间的通信进行保护。
- 将 ACL 中源、目的 IP 地址与建立 GRE 隧道的源、目的 IP 地址配置不相同，并将策略应用在隧道接口下，可以对通过 GRE 隧道的部分数据流进行保护。

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

- 要将所有的 IPsec 策略都绑定在对应的 GRE 接口上；
- 所有的出接口 Ethernet0/0 都不使能 OSPF，且必须保证总部和分支出接口能互通；
- ACL 一定不要最后添加一条 deny ip 的规则，该配置会导致不需要加密的流量被丢弃。

3.5 配置步骤

3.5.1 Router A的配置

配置接口 Ethernet0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface ethernet 0/1
[RouterA-Ethernet0/1] ip address 10.0.0.1 255.255.255.0
[RouterA-Ethernet0/1] quit
```

配置接口 Ethernet0/0 的 IP 地址。

```
[RouterA] interface ethernet 0/0
[RouterA-Ethernet0/0] ip address 1.0.0.254 255.255.255.0
[RouterA-Ethernet0/0] quit
```

配置 OSPF Router ID 的 Loopback 接口地址。

```
[RouterA] interface loopback 0
[RouterA-LoopBack0] ip address 192.168.255.255 255.255.255.255
[RouterA-LoopBack0] quit
```

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 ethernet 0/0
[RouterA-Tunnel0] destination 1.0.0.1
[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 ethernet 0/0
[RouterA-Tunnel1] destination 1.0.0.2
[RouterA-Tunnel1] quit
```
配置 OSPF 路由协议。
```
[RouterA] router id 192.168.255.255
[RouterA] ospf 1
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.0.0.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 192.168.255.255 0.0.0.0
[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
```
创建 ACL3000,定义与 branch1 之间需要 IPsec 保护的数据流。
```
[RouterA] acl number 3000
[RouterA-acl-adv-3000] rule 0 permit ip source 10.0.0.0 0.255.255.255 destination
 192.168.1.0 0.0.0.255
[RouterA-acl-adv-3000] quit
```
创建 ACL3001,定义与 branch2 之间需要 IPsec 保护的数据流。
```
[RouterA] acl number 3001
[RouterA-acl-adv-3001] rule 0 permit ip source 10.0.0.0 0.255.255.255 destination
 192.168.2.0 0.0.0.255
[RouterA-acl-adv-3001] quit
```
配置 IKE 对等体 branch1。
```
[RouterA] ike peer branch1
[RouterA-ike-peer-branch1] pre-shared-key 123
[RouterA-ike-peer-branch1] remote-address 192.168.0.2
[RouterA-ike-peer-branch1] quit
```
配置 IKE 对等体 branch2。
```
[RouterA] ike peer branch2
[RouterA-ike-peer-branch2] pre-shared-key 123
[RouterA-ike-peer-branch2] remote-address 192.168.0.6
[RouterA-ike-peer-branch2] quit
```
采用安全提议的缺省配置。
```
[RouterA] ipsec transform-set 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 branch1，其协商方式为 isakmp。
```
[RouterA] ipsec policy branch1 1 isakmp
[RouterA-ipsec-policy-isakmp-branch1-1] security acl 3000
[RouterA-ipsec-policy-isakmp-branch1-1] ike-peer branch1
[RouterA-ipsec-policy-isakmp-branch1-1] transform-set def
[RouterA-ipsec-policy-isakmp-branch1-1] quit
```

创建 IPsec 安全策略 branch2，其协商方式为 isakmp。

```
[RouterA] ipsec policy branch2 1 isakmp
[RouterA-ipsec-policy-isakmp-branch2-1] security acl 3001
[RouterA-ipsec-policy-isakmp-branch2-1] ike-peer branch2
[RouterA-ipsec-policy-isakmp-branch2-1] transform-set def
[RouterA-ipsec-policy-isakmp-branch2-1] quit
```

在 GRE 接口上应用安全策略。

```
[RouterA] interface tunnel 0
[RouterA-Tunnel0] ipsec policy branch1
[RouterA-Tunnel0] quit
[RouterA] interface tunnel 1
[RouterA-Tunnel1] ipsec policy branch2
[RouterA-Tunnel1] quit
```

3.5.2 Router B的配置

配置接口 Ethernet0/1 的 IP 地址。

```
<RouterB> system-view
[RouterB] interface ethernet 0/1
[RouterB-Ethernet0/1] ip address 192.168.1.1 255.255.255.0
[RouterB-Ethernet0/1] quit
```

配置接口 Ethernet0/0 的 IP 地址。

```
[RouterB]interface ethernet 0/0
[RouterB-Ethernet0/0] ip address 1.0.0.1 255.255.255.0
[RouterB-Ethernet0/0] quit
```

配置 OSPF Router ID 的 Loopback 接口地址。

```
[RouterB] interface loopback 0
[RouterB-LoopBack0] ip address 192.168.255.1 255.255.255.255
[RouterB-LoopBack0] quit
```

配置到 center 的 GRE 隧道。

```
[RouterB] interface tunnel 0
[RouterB-Tunnel0] ip address 192.168.0.2 255.255.255.252
[RouterB-Tunnel0] source ethernet 0/0
[RouterB-Tunnel0] destination 1.0.0.254
[RouterB-Tunnel0] quit
```

配置 OSPF 路由协议。

```
[RouterB] router id 192.168.255.1
[RouterB] ospf 1
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.255.1 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.3
[RouterB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
```

创建 ACL3000,定义需要 IPsec 保护的数据流。

```
[RouterB] acl number 3000
[RouterB-acl-adv-3000] rule 0 permit ip source 192.168.1.0 0.0.0.255 destination
```

```
10.0.0.0 0.0.0.255
[RouterB-acl-adv-3000] quit
```
配置 IKE 对等体 center。
```
[RouterB] ike peer center
[RouterB-ike-peer-center] pre-shared-key 123
[RouterB-ike-peer-center] remote-address 192.168.0.1
[RouterB-ike-peer-center] quit
```
采用安全提议的缺省配置。
```
[RouterB] ipsec transform-set def
```
配置 ESP 协议采用 md5 认证算法。
```
[RouterB-ipsec-transform-set-def] esp authentication-algorithm md5
[RouterB-ipsec-transform-set-def] quit
```
创建 IPsec 安全策略 center，其协商方式为 isakmp。
```
[RouterB] ipsec policy center 1 isakmp
[RouterB-ipsec-policy-isakmp-center-1] security acl 3000
[RouterB-ipsec-policy-isakmp-center-1] ike-peer center
[RouterB-ipsec-policy-isakmp-center-1] transform-set def
[RouterB-ipsec-policy-isakmp-center-1] quit
```
在 GRE 接口上应用安全策略。
```
[RouterB] interface tunnel 0
[RouterB-Tunnel0] ipsec policy center
[RouterB-Tunnel0] quit
```

3.5.3 Router C的配置

配置接口 Ethernet0/1 的 IP 地址。
```
<RouterC> system-view
[RouterC] interface ethernet 0/1
[RouterC-Ethernet0/1] ip address 192.168.2.1 255.255.255.0
[RouterC-Ethernet0/1] quit
```
配置接口 Ethernet0/0 的 IP 地址。
```
[RouterC] interface ethernet 0/0
[RouterC-Ethernet0/0] ip address 1.0.0.2 255.255.255.0
[RouterC-Ethernet0/0] quit
```
配置 OSPF Router ID 的 Loopback 接口地址。
```
[RouterC] interface loopback 0
[RouterC-LoopBack0] ip address 192.168.255.2 255.255.255.255
[RouterC-LoopBack0] quit
```
配置到 center 的 GRE 隧道。
```
[RouterC] interface tunnel 0
[RouterC-Tunnel0] ip address 192.168.0.6 255.255.255.252
[RouterC-Tunnel0] source ethernet 0/0
[RouterC-Tunnel0] destination 1.0.0.254
[RouterC-Tunnel0] quit
```
配置 OSPF 路由协议。

```
[RouterC] router id 192.168.255.2
[RouterC] ospf 1
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 192.168.255.2 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 192.168.0.4 0.0.0.3
[RouterC-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
```

创建 ACL3000,定义需要 IPsec 保护的数据流。

```
[RouterC] acl number 3000
[RouterC-acl-adv-3000] rule 0 permit ip source 192.168.2.0 0.0.0.255 destination
10.0.0.0 0.255.255.255
[RouterC-acl-adv-3000] quit
```

配置 IKE 对等体 center。

```
[RouterC] ike peer center
[RouterC-ike-peer-center] pre-shared-key 123
[RouterC-ike-peer-center] remote-address 192.168.0.5
[RouterC-ike-peer-center] quit
```

采用安全提议的缺省配置。

```
[RouterC] ipsec transform-set def
```

配置 ESP 协议采用 md5 认证算法。

```
[RouterC-ipsec-transform-set-def] esp authentication-algorithm md5
[RouterC-ipsec-transform-set-def] quit
```

创建 IPsec 安全策略 center，其协商方式为 isakmp。

```
[RouterC] ipsec policy center 1 isakmp
[RouterC-ipsec-policy-isakmp-center-1] security acl 3000
[RouterC-ipsec-policy-isakmp-center-1] ike-peer center
[RouterC-ipsec-policy-isakmp-center-1] transform-set def
[RouterC-ipsec-policy-isakmp-center-1] quit
```

在 GRE 接口上应用安全策略。

```
[RouterC] interface tunnel 0
[RouterC-Tunnel0] ipsec policy center
[RouterC-Tunnel0] quit
```

3.6 验证配置

完成以上配置后，总部与分支的所有内网之间可以互通，且只有 ACL 定义的流量被加密。

这里以 Router B 为例进行验证，Router A 和 Router B 验证方法相同。

通过以下显示信息可以看到，Router B 和 Router C 的内网之间可以互通。

```
<RouterB> ping -a 192.168.1.1 192.168.2.1
PING 192.168.2.1: 56  data bytes, press CTRL_C to break
  Reply from 192.168.2.1: bytes=56 Sequence=0 ttl=254 time=3 ms
  Reply from 192.168.2.1: bytes=56 Sequence=1 ttl=254 time=2 ms
  Reply from 192.168.2.1: bytes=56 Sequence=2 ttl=254 time=2 ms
  Reply from 192.168.2.1: bytes=56 Sequence=3 ttl=254 time=2 ms
  Reply from 192.168.2.1: bytes=56 Sequence=4 ttl=254 time=3 ms
```

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

通过以下显示信息可以看到，由于 Router B 和 Router C 内网的流量不属于 ACL 定义的需加密的流量，因此，不能触发 IPsec。

```
<RouterB> dis ike sa
    total phase-1 SAs:  0
    connection-id  peer                    flag        phase   doi
  ----------------------------------------------------------------

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT RK--REKEY
<RouterB> dis ipsec sa
```

通过以下显示信息可以看到，Router B 和 Router A 之间的内网之间可以互通。

```
<RouterB> ping -a 192.168.1.1 10.0.0.1
  PING 10.0.0.1: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 10.0.0.1: bytes=56 Sequence=1 ttl=255 time=3 ms
    Reply from 10.0.0.1: bytes=56 Sequence=2 ttl=255 time=3 ms
    Reply from 10.0.0.1: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 10.0.0.1: bytes=56 Sequence=4 ttl=255 time=2 ms

  --- 10.0.0.1 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
round-trip min/avg/max = 2/2/3 ms
```

由于 Router B 和 Router A 内网的流量已在 ACL 中定义为需加密保护的流量，因此将触发 IPsec 进行加密。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。

```
<RouterB> display ike sa
    total phase-1 SAs:  1
    connection-id  peer                    flag        phase   doi
  ----------------------------------------------------------------
     1             192.168.0.1             RD|ST       1       IPSEC
     2             192.168.0.1             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。

```
<RouterB> display ipsec sa
==============================
Interface: Tunnel0
    path MTU: 1476
==============================
```

```
  ----------------------------
  IPsec policy name: "center"
  sequence number: 1
  acl version: ACL4
  mode: isakmp
  ----------------------------
    PFS: N, DH group: none
    tunnel:
        local  address: 192.168.0.2
        remote address: 192.168.0.1
    flow:
        sour addr: 192.168.1.0/255.255.255.0  port: 0  protocol: IP
        dest addr: 10.0.0.0/255.255.255.0  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 0xD37AE9A4(3548047780)
      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): 1843199/3539
      anti-replay detection: Enabled
        anti-replay window size(counter based): 32
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 0x86700DE2(2255490530)
      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): 1843199/3539
      anti-replay detection: Enabled
        anti-replay window size(counter based): 32
      udp encapsulation used for nat traversal: N
```

可以通过如下显示信息查看 GRE 隧道的建立情况。

```
<RouterB> 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 1.0.0.1 (Ethernet0/0), destination 1.0.0.254
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:  8 bytes/sec, 0 packets/sec
    Last 300 seconds output:  8 bytes/sec, 0 packets/sec
    184 packets input,  13716 bytes
    0 input error
    174 packets output,  12812 bytes
    0 output error
```

可以通过如下显示信息查看 OSPF 路由表和邻居建立情况。

```
<RouterB> display ospf routing

          OSPF Process 1 with Router ID 192.168.255.1
                  Routing Tables

 Routing for Network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 192.168.255.255/32 1562     Stub    192.168.0.1     192.168.255.255 0.0.0.0
 10.0.0.1/32        1562     Stub    192.168.0.1     192.168.255.255 0.0.0.0
 192.168.0.0/30     1562     Stub    192.168.0.2     192.168.255.1   0.0.0.0
 192.168.0.4/30     3124     Stub    192.168.0.1     192.168.255.255 0.0.0.0
 192.168.1.1/32     0        Stub    192.168.1.1     192.168.255.1   0.0.0.0
 192.168.2.1/32     3124     Stub    192.168.0.1     192.168.255.2   0.0.0.0
 192.168.255.1/32   0        Stub    192.168.255.1   192.168.255.1   0.0.0.0
 192.168.255.2/32   3124     Stub    192.168.0.1     192.168.255.2   0.0.0.0

 Total Nets: 8
 Intra Area: 8  Inter Area: 0  ASE: 0  NSSA: 0

<RouterB> display ospf lsdb

          OSPF Process 1 with Router ID 192.168.255.1
                  Link State Database

                          Area: 0.0.0.0
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    192.168.255.255 192.168.255.255   1281  96    80000006       0
 Router    192.168.255.2   192.168.255.2     1266  72    80000004       0
 Router    192.168.255.1   192.168.255.1     1355  72    80000004       0

<RouterB> display ospf peer

                  OSPF Process 1 with Router ID 192.168.255.1
                       Neighbor Brief Information
```

```
 Area: 0.0.0.0
 Router ID       Address         Pri  Dead-Time  Interface       State
 192.168.255.255 192.168.0.1     1    31         Tun0            Full/ -
```

3.7 配置文件

- Router A：

```
#
 router id 192.168.255.255
#
acl number 3000
 rule 0 permit ip source 10.0.0.0 0.255.255.255 destination 192.168.1.0 0.0.0.25
5
acl number 3001
 rule 0 permit ip source 10.0.0.0 0.255.255.255 destination 192.168.2.0 0.0.0.25
5
#
ike peer branch1
 pre-shared-key cipher $c$3$Hrwy5G5GJ4yA62gpcP5+JqEtifSvmw==
 remote-address 192.168.0.2
#
ike peer branch2
 pre-shared-key cipher $c$3$wogCOxJn/Yt9/Ix/bpcub18oq0kLXA==
 remote-address 192.168.0.6
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy branch1 1 isakmp
 security acl 3000
 ike-peer branch1
 transform-set def
#
ipsec policy branch2 1 isakmp
 security acl 3001
 ike-peer branch2
 transform-set def
#
interface Ethernet0/1
 port link-mode route
 ip address 10.0.0.1 255.255.255.0
#
interface Ethernet0/0
 port link-mode route
 ip address 1.0.0.254 255.255.255.0
#
```

```
interface LoopBack0
 ip address 192.168.255.255 255.255.255.255
#
interface Tunnel0
 ip address 192.168.0.1 255.255.255.252
 source Ethernet0/0
 destination 1.0.0.1
 ipsec policy branch1
#
interface Tunnel1
 ip address 192.168.0.5 255.255.255.252
 source Ethernet0/0
 destination 1.0.0.2
 ipsec policy branch2
#
ospf 1
 area 0.0.0.0
  network 10.0.0.0 0.0.0.255
  network 192.168.255.255 0.0.0.0
  network 192.168.0.0 0.0.0.3
  network 192.168.0.4 0.0.0.3
#
```

- Router B：

```
#
 router id 192.168.255.1
#
acl number 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 10.0.0.0 0.0.0.255
#
ike peer center
 pre-shared-key cipher $c$3$pR4XoeELsbjG9RfWfrm5GT3Ro3EsOQ==
 remote-address 192.168.0.1
#
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 Ethernet0/1
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
#
interface Ethernet0/0
```

```
 port link-mode route
 ip address 1.0.0.1 255.255.255.0
#
interface LoopBack0
 ip address 192.168.255.1 255.255.255.255
#
interface Tunnel0
 ip address 192.168.0.2 255.255.255.252
 source Ethernet0/0
 destination 1.0.0.254
 ipsec policy center
#
ospf 1
 area 0.0.0.0
  network 192.168.255.1 0.0.0.0
  network 192.168.0.0 0.0.0.3
  network 192.168.1.0 0.0.0.255
#
```

- Router C：

```
#
 router id 192.168.255.2
#
acl number 3000
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 10.0.0.0 0.255.255.25
5
#
ike peer center
 pre-shared-key cipher $c$3$b/tFRG/i1Mg/80d4fZWThzLcNzcVag==
 remote-address 192.168.0.5
#
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 Ethernet0/1
 port link-mode route
 ip address 192.168.2.1 255.255.255.0
#
interface Ethernet0/0
 port link-mode route
 ip address 1.0.0.2 255.255.255.0
#
```

```
interface LoopBack0
 ip address 192.168.255.2 255.255.255.255
#
interface Tunnel0
 ip address 192.168.0.6 255.255.255.252
 source Ethernet0/0
 destination 1.0.0.254
 ipsec policy center
#
ospf 1
 area 0.0.0.0
  network 192.168.255.2 0.0.0.0
  network 192.168.0.4 0.0.0.3
  network 192.168.2.0 0.0.0.255
#
```

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