

## 组网及说明

### 1 配置需求或说明

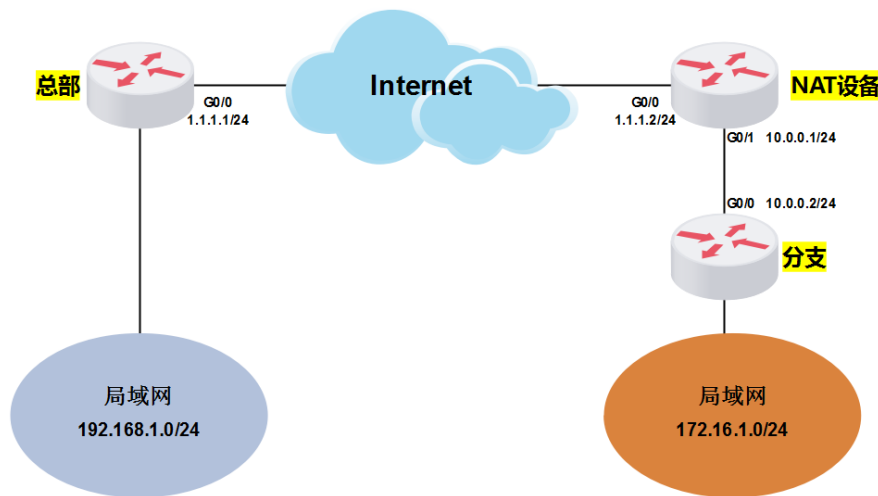
#### 1.1 适用产品系列

本案例适用于如MSR800、MSR830、MSR900、MSR900E、MSR930等MSR800、MSR830、MSR900、MSR930系列的路由器。

#### 1.2 配置需求及实现的效果

总部路由器外网口为地址1.1.1.1（模拟运营商公网固定地址环境），分支路由器前面有NAT设备，分支路由器作为二级路由由外网口地址为私网地址10.0.0.2（模拟运营商非公网地址环境），要实现总部路由器的局域网网段（192.168.1.0/24）和分支路由器的局域网网段（172.16.1.0/24）互访。

### 2 组网图



## 配置步骤

### 3 配置步骤

#### 3.1 配置路由器基本上网

#路由器基本上网配置省略，具体设置步骤请参考“2.1.2 路由器外网使用固定IP地址上网配置方法”章节中“MSR830[930][2600]系列路由器基本上网（静态IP）WEB配置（V5）”案例

#### 3.2 配置总部IPSEC VPN

```
system-view
```

```
#配置公网口NAT要关联的ACL 3000，作用是把IPSec感兴趣流从NAT转换的数据流deny掉
```

```
[H3C]acl number 3000
```

```
[H3C-acl-adv-3000]rule 0 deny ip source 192.168.1.0 0.0.0.255 destination 172.16.1.0 0.0.0.255
```

```
[H3C-acl-adv-3000]rule 5 permit ip
```

```
#配置IPSec感兴趣流ACL 3333，匹配源地址为总部内网网段目的地址为分支内网网段的数据流
```

```
[H3C-acl-adv-3000]acl number 3333
```

```
[H3C-acl-adv-3333]rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 172.16.1.0 0.0.0.255
```

```
[H3C-acl-adv-3333]quit
```

```
#配置本端安全网关的名字为zongbu
```

```
[H3C]ike local-name zongbu
```

```
#创建IKE对等体123，IKE阶段的协商模式为野蛮模式，IKE预共享密钥为123456，配置名字作为IKE协商过程中使用的ID（缺省情况下，使用IP地址作为IKE协商过程中使用的ID），配置对端网关的名字为fenzhi（要与对端的ike local-name配置对应），并开启NAT穿越功能
```

```
[H3C]ike peer 123
```

```
[H3C-ike-peer-123]exchange-mode aggressive
```

```
[H3C-ike-peer-123]pre-shared-key simple 123456
```

```
[H3C-ike-peer-123]id-type name
```

```
[H3C-ike-peer-123]remote-name fenzhi
```

```
[H3C-ike-peer-123]nat traversal
```

```
[H3C-ike-peer-123]quit
```

```
#创建IPSec安全提议123，配置ESP协议采用的认证算法为sha1，加密算法为3des
```

```

[H3C]ipsec transform-set 123
[H3C-ipsec-transform-set-123]esp authentication-algorithm sha1
[H3C-ipsec-transform-set-123]esp encryption-algorithm 3des
[H3C-ipsec-transform-set-123]quit
#创建IPSec安全策略123，引用之前创建的ACL 3333，引用之前创建的对等体123，引用之前创建的
Psec安全提议123
[H3C]ipsec policy 123 1 isakmp
[H3C-ipsec-policy-isakmp-123-1]security acl 3333
[H3C-ipsec-policy-isakmp-123-1]ike-peer 123
[H3C-ipsec-policy-isakmp-123-1]transform-set 123
[H3C-ipsec-policy-isakmp-123-1]quit
#设置外网口做NAT转换的时候关联ACL 3000（如果之前已经在外网口配置了 nat outbound，需要先
undo掉），并将IPSec安全策略123应用在外网接口
[H3C]interface GigabitEthernet0/0
[H3C-GigabitEthernet0/0]undo nat outbound
[H3C-GigabitEthernet0/0]nat outbound 3000
[H3C-GigabitEthernet0/0]ip address 1.1.1.1 255.255.255.0
[H3C-GigabitEthernet0/0]ipsec policy 123
[H3C-GigabitEthernet0/0]quit

```

### 3.3 配置分部路由器IPSEC

```

system-view
#配置公网口NAT要关联的ACL 3000，作用是把IPSec感兴趣流从NAT转换的数据流deny掉
[H3C]acl number 3000
[H3C-acl-adv-3000]rule 0 deny ip source 172.16.1.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
[H3C-acl-adv-3000]rule 5 permit ip
#配置IPSec感兴趣流ACL 3333，匹配源地址为分支内网网段，目的地址为总部内网网段的数据流
[H3C]acl number 3333
[H3C-acl-adv-3333]rule 0 permit ip source 172.16.1.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
[H3C-acl-adv-3333]quit
#配置本端安全网关的名字为fenzhi
[H3C]ike local-name fenzhi
#创建IKE对等体123，IKE阶段的协商模式为野蛮模式，IKE预共享密钥为123456，配置名字作为IKE
协商过程中使用的ID（缺省情况下，使用IP地址作为IKE协商过程中使用的ID），配置对端网关的名字
为zongbu（要与对端的ike local-name配置对应），配置对端网关的地址为1.1.1.1，并开启NAT穿越功
能
[H3C]ike peer 123
[H3C-ike-peer-123]exchange-mode aggressive
[H3C-ike-peer-123]pre-shared-key simple 123456
[H3C-ike-peer-123]id-type name
[H3C-ike-peer-123]remote-name zongbu
[H3C-ike-peer-123]remote-address 1.1.1.1
[H3C-ike-peer-123]nat traversal
[H3C-ike-peer-123]quit
创建IPSec安全提议123，配置ESP协议采用的认证算法为sha1，加密算法为3des
[H3C]ipsec transform-set 123
[H3C-ipsec-transform-set-123]esp authentication-algorithm sha1
[H3C-ipsec-transform-set-123]esp encryption-algorithm 3des
[H3C-ipsec-transform-set-123]quit
#创建IPSec安全策略123，引用之前创建的ACL 3333，引用之前创建的对等体123，引用创建的IPSec
安全提议123
[H3C]ipsec policy 123 1 isakmp
[H3C-ipsec-policy-isakmp-123-1]security acl 3333
[H3C-ipsec-policy-isakmp-123-1]ike-peer 123
[H3C-ipsec-policy-isakmp-123-1]transform-set 123
[H3C-ipsec-policy-isakmp-123-1]quit
#设置外网口做NAT转换的时候关联ACL 3000（如果之前已经在外网口配置了 nat outbound，需要先
undo掉），并将IPSec安全策略123应用在外网接口
[H3C]interface GigabitEthernet0/0
[H3C-GigabitEthernet0/0]undo nat outbound
[H3C-GigabitEthernet0/0]nat outbound 3000
[H3C-GigabitEthernet0/0] ip address 10.0.0.2 255.255.255.0
[H3C-GigabitEthernet0/0] ipsec policy 123
[H3C-GigabitEthernet0/0]quit

```

### 3.4 验证配置结果

#在分支MSR路由器上带源ping总部MSR路由器内网网关地址

```
<H3C>ping -a 172.16.1.1 192.168.1.1
PING 192.168.1.1: 56 data bytes, press CTRL_C to break
Request time out
Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=255 time=1 ms
Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=255 time=2 ms
Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms

--- 192.168.1.1 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 1/1/2 ms
```

#在分支MSR路由器上查看IKE SA和IPSec SA的状态，可以看到IKE SA和IPSec SA均已正常建立。

```
<H3C>display ike sa
total phase-1 SAs: 1
connection-id peer flag phase doi
-----
 29 1.1.1.1 RD|ST 1 IPSEC
 30 1.1.1.1 RD|ST 2 IPSEC

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

```
<H3C>display ipse sa
=====
Interface: GigabitEthernet0/0
path MTU: 1500
=====

-----
IPsec policy name: "123"
sequence number: 1
acl version: ACL4
mode: isakmp
-----

PFS: N, DH group: none
inside VRF:
tunnel:
  local address: 10.0.0.2
  remote address: 1.1.1.1
flow:
  sour addr: 172.16.1.0/255.255.255.0 port: 0 protocol: IP
  dest addr: 192.168.1.0/255.255.255.0 port: 0 protocol: IP

[inbound ESP SAs]
spi: 0x70EE52C3(1894666947)
transform: ESP-ENCRYPT-3DES ESP-AUTH-SHA1
in use setting: Tunnel
connection id: 51
sa duration (kilobytes/sec): 1843200/3600
sa remaining duration (kilobytes/sec): 1843199/1300
anti-replay detection: Enabled
  anti-replay window size(counter based): 32
udp encapsulation used for nat traversal: Y

[outbound ESP SAs]
spi: 0x5DD34B21(1574128417)
transform: ESP-ENCRYPT-3DES ESP-AUTH-SHA1
in use setting: Tunnel
connection id: 52
sa duration (kilobytes/sec): 1843200/3600
sa remaining duration (kilobytes/sec): 1843199/1300
anti-replay detection: Enabled
  anti-replay window size(counter based): 32
udp encapsulation used for nat traversal: Y
```

配置关键点