# MSR 系列路由器一端固定 IP，另一端拨号动态获取地址的 IPsec 通信配置举例

# 目 录

1 简介 ..... 1
2 配置前提 ..... 1
3 配置举例 ..... 1
3.1 组网需求 ..... 1
3.2 配置思路 ..... 1
3.3 使用版本 ..... 1
3.4 配置步骤 ..... 2
3.4.1 Router A的配置 ..... 2
3.4.2 Router B的配置 ..... 3
3.5 验证配置 ..... 4
3.6 配置文件 ..... 6
4 相关资料 ..... 8

# 1 简介

本文档介绍MSR系列路由器一端固定IP，另一端拨号动态获取地址的IPsec通信的典型配置案例。

# 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。

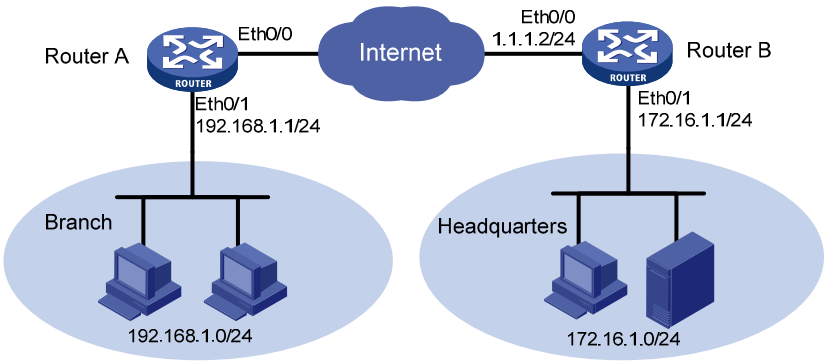
本文档假设您已了解 IPsec 和 PPP 的特性。

# 3 配置举例

## 3.1 组网需求

如 图 1 所示，Router A为企业分支网关，Router B为企业总部网关。企业分支使用拨号方式获取动态IP地址接入Internet，企业总部使用固定的IP地址接入Internet。要求基于ACL采用IKE方式建立IPsec安全隧道，对分支子网与总部子网之间的所有数据流进行安全保护。

图1 一端固定 IP，另一端拨号动态获取地址的 IPsec 通信配置组网图




## 3.2 配置思路

- 为了让Router A使用拨号方式获取动态IP地址接入Internet，需要将Router A配置成PPPoE Client。
- 为了让受保护的流量触发安全策略，需要对 Router A 和 Router B 配置不对 IPsec 数据流进行 NAT 转换。

## 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 配置步骤

### 3.4.1 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 192.168.1.1 255.255.255.0
[RouterA-Ethernet0/1] quit
```

# 配置 NAT 转换的 ACL。

```
[RouterA] acl number 2000
[RouterA-acl-basic-2000] rule 0 permit
[RouterA-acl-basic-2000] quit
```

# 配置 ACL，定义由 192.168.1.0/24 到 172.16.1.0/24 的数据流。

```
[RouterA] acl number 3000
[RouterA-acl-adv-3000] rule 0 permit ip source 192.168.1.0 0.0.0.255 destination
172.16.1.0 0.0.0.255
[RouterA-acl-adv-3000] quit
```

# 创建一个 IKE 对等体，并进入 IKE-Peer 视图。

```
[RouterA] ike peer peer
```

# 配置 IKE 第一阶段的协商模式为野蛮模式。

```
[RouterA-ike-peer-peer] exchange-mode aggressive
```

# 配置预共享密钥。

```
[RouterA-ike-peer-peer] pre-shared-key 123
```

# 配置对端安全网关 IP 地址。

```
[RouterA-ike-peer-peer] remote-address 1.1.1.2
```

# 启用 NAT 穿越功能。

```
[RouterA-ike-peer-peer] nat traversal
[RouterA-ike-peer-peer] 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 policy，其协商方式为 isakmp。

```
[RouterA] ipsec policy policy 1 isakmp
```

# 配置 IPsec 安全策略引用的访问控制列表。

```
[RouterA-ipsec-policy-isakmp-policy-1] security acl 3000
```

# 在 IPsec 安全策略中引用 IKE 对等体。

```
[RouterA-ipsec-policy-isakmp-policy-1] ike-peer peer
```

# 配置 IPsec 安全策略所引用的 IPsec 安全提议。

```
[RouterA-ipsec-policy-isakmp-policy-1] proposal def
[RouterA-ipsec-policy-isakmp-policy-1] quit
```

# 对从企业分支网络出来的所有报文作 NAT 转换。

```
[RouterA] interface dialer 0
[RouterA-Dialer0] nat outbound 2000
[RouterA-Dialer0] link-protocol ppp
```

# 配置 ppp 验证的用户名。

```
[RouterA-Dialer0] ppp chap user test
```

# 配置 ppp 验证的密码。

```
[RouterA-Dialer0] ppp chap password simple test
```

# 本端口 IP 地址由 ppp 协商获得。

```
[RouterA-Dialer0] ip address ppp-negotiate
```

# 配置拨号用户为 pppoe。

```
[RouterA-Dialer0] dialer user pppoe
```

# 配置拨号捆绑，用于绑定物理接口。

```
[RouterA-Dialer0] dialer bundle 1
```

# 配置不对 IPsec 数据流进行 NAT 转换。

```
[RouterA-Dialer0] ipsec no-nat-process enable
```

# 在接口上应用安全策略。

```
[RouterA-Dialer0] ipsec policy policy
[RouterA-Dialer0] quit
```

# 配置 PPPoE 会话。

```
[RouterA] interface ethernet 0/0
[RouterA-Ethernet0/0] pppoe-client dial-bundle-number 1
[RouterA-Ethernet0/0] quit
```

# 配置到总部网络的静态路由。

```
[RouterA] ip route-static 172.16.1.0 255.255.255.0 dialer 0
```

### 3.4.2 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 172.16.1.1 255.255.255.0
[RouterB-Ethernet0/1] quit
```

# 配置 NAT 转换的 ACL。

```
[RouterB] acl number 2000
[RouterB-acl-basic-2000] rule 0 permit
[RouterB-acl-basic-2000] quit
```

# 配置 ACL，定义由 172.16.1.0/24 到 192.168.1.0/24 的数据流。

```
[RouterB] acl number 3000
[RouterB-acl-adv-3000] rule 0 permit ip source 172.16.1.0 0.0.0.255
destination 192.168.1.0 0.0.0.255
[RouterB-acl-adv-3000] quit
```

# 创建一个 IKE 对等体，并进入 IKE-Peer 视图。

```
[RouterB] ike peer peer
```
# 配置 IKE 第一阶段的协商模式为野蛮模式。
```
[RouterB-ike-peer-peer] exchange-mode aggressive
```
# 配置预共享密钥。
```
[RouterB-ike-peer-peer] pre-shared-key 123
```
# 启用 NAT 穿越功能。
```
[RouterB-ike-peer-peer] nat traversal
[RouterB-ike-peer-peer] quit
```
# 采用安全提议的缺省配置。
```
[RouterB] 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
```
# 创建一个 IPsec 安全策略模板，并进入 IPsec 安全策略模板视图。
```
[RouterB] ipsec policy-template test 1
```
# 配置 IPsec 安全策略引用的访问控制列表。
```
[RouterB-ipsec-policy-isakmp-policy-1] security acl 3000
```
# 在 IPsec 安全策略中引用 IKE 对等体。
```
[RouterB-ipsec-policy-template-test-1] ike-peer peer
```
# 配置 IPsec 安全策略所引用的 IPsec 安全提议。
```
[RouterB-ipsec-policy-template-test-1] proposal def
[RouterB-ipsec-policy-template-test-1] quit
```
# 引用 IPsec 安全策略模板创建一条 IPsec 安全策略。
```
[RouterB] ipsec policy policy 1 isakmp template test
```
# 对从企业总部网络出来的所有报文作 NAT 转换。
```
[RouterB] interface ethernet 0/0
[RouterB-Ethernet0/0] nat outbound 2000
[RouterB-Ethernet0/0] ip address 1.1.1.2 255.255.255.0
```
# 配置不对 Ipsec 数据流进行 NAT 转换。
```
[RouterB-Ethernet0/0] ipsec no-nat-process enable
```
# 在接口上应用安全策略。
```
[RouterB-Ethernet0/0] ipsec policy policy
[RouterB-Ethernet0/0] quit
```
# 配置到分支网络的静态路由，下一跳指向上行网关地址。
```
[RouterB] ip route-static 192.168.1.0 255.255.255.0 1.1.1.1
```

## 3.5 验证配置

以上配置完成之后，当 Router A 的接口 Ethernet0/0 完成自动拨号后，Router A 会自动发起与 Router B 之间的 IKE 协商。当 IKE 协商完成之后，Router A 和 Router B 即可满足组网需求，对总部和分支的数据流进行安全保护。这里以 Router A 为例进行验证，Router B 的验证方法相同。

# 在 Router A 上可以 ping 通 Router B 连接的总部私网地址。
```
<RouterA> ping -a 192.168.1.1 172.16.1.1
```

```
  PING 172.16.1.1: 56  data bytes, press CTRL_C to break
    Reply from 172.16.1.1: bytes=56 Sequence=0 ttl=255 time=3 ms
    Reply from 172.16.1.1: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 172.16.1.1: bytes=56 Sequence=2 ttl=255 time=3 ms
    Reply from 172.16.1.1: bytes=56 Sequence=3 ttl=255 time=3 ms
    Reply from 172.16.1.1: bytes=56 Sequence=4 ttl=255 time=3 ms

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

# 可以通过如下显示信息看到，Router A 作为发起方已与 Router B 协商生成了两个阶段的 SA。

```
<RouterA> display ike sa
    total phase-1 SAs:  1
    connection-id  peer                    flag        phase   doi
  --------------------------------------------------------------------
     24            1.1.1.2                 RD|ST       1       IPSEC
     25            1.1.1.2                 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。

```
<RouterA> display ipsec sa
==============================
Interface: Ethernet0/0
    path MTU: 1500
==============================

  ----------------------------
  IPsec policy name: "policy"
  sequence number: 1
  acl version: ACL4
  mode: isakmp
  ----------------------------
    PFS: N, DH group: none
    tunnel:
        local  address: 1.1.1.1
        remote address: 1.1.1.2
    flow:
        sour addr: 192.168.1.0/255.255.255.0  port: 0  protocol: IP
        dest addr: 172.16.1.0/255.255.255.0  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 0xBACB0D56(3133869398)
      transform: ESP-ENCRYPT-NULL ESP-AUTH-MD5
      in use setting: Tunnel
      connection id: 13
```

```
    sa duration (kilobytes/sec): 1843200/3600
    sa remaining duration (kilobytes/sec): 1843197/2926
    anti-replay detection: Enabled
      anti-replay window size(counter based): 32
    udp encapsulation used for nat traversal: N

  [outbound ESP SAs]
    spi: 0x93DE082E(2480801838)
    transform: ESP-ENCRYPT-NULL ESP-AUTH-MD5
    in use setting: Tunnel
    connection id: 14
    sa duration (kilobytes/sec): 1843200/3600
    sa remaining duration (kilobytes/sec): 1843197/2926
    anti-replay detection: Enabled
      anti-replay window size(counter based): 32
    udp encapsulation used for nat traversal: N
```

## 3.6 配置文件

- Router A：

```
#
acl number 2000
 rule 0 permit
#
acl number 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 172.16.1.0 0.0.0.255
#
ike peer peer
 exchange-mode aggressive
 pre-shared-key cipher $c$3$ujchwj2Y0H7X45rl8VZSmol8HAg6kQ==
 remote-address 1.1.1.2
 nat traversal
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy policy 1 isakmp
 security acl 3000
 ike-peer peer
 transform-set def
#
interface Dialer0
 nat outbound 2000
 link-protocol ppp
 ppp chap user test
 ppp chap password cipher $c$3$gm+SloptI6+UO5ySMAmh/b1rnuooeko=
```

```
 ip address ppp-negotiate
 dialer user pppoe
 dialer bundle 1
 ipsec no-nat-process enable
 ipsec policy policy
#
interface Ethernet0/1
 port link-mode route
ip address 192.168.1.1 255.255.255.0
#
interface Ethernet0/0
 port link-mode route
pppoe-client dial-bundle-number 1
#
ip route-static 172.16.1.0 255.255.255.0 Dialer0
#
```

- Router B：

```
#
acl number 2000
 rule 0 permit
#
acl number 3000
 rule 0 permit ip source 172.16.1.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ike peer peer
 exchange-mode aggressive
 pre-shared-key cipher $c$3$vsR5A5bYPmC0vnVTvs6KfkR2rjTpfw==
 nat traversal
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy-template test 1
 ike-peer peer
 transform-set def
#
ipsec policy policy 1 isakmp template test
#
interface Ethernet0/1
 port link-mode route
ip address 172.16.1.1 255.255.255.0
#
interface Ethernet0/0
 port link-mode route
nat outbound 2000
 ip address 1.1.1.2 255.255.255.0
```

```
 ipsec no-nat-process enable
 ipsec policy policy
#
ip route-static 192.168.1.0 255.255.255.0 1.1.1.1
#
```

# 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