MSR 系列路由器 IPsec VPN 多分支安全模板 NAT 穿越功能的配置举例

目 录

1 简介

本文档介绍 MSR 路由器 IPsec VPN 多分支安全模板 NAT 穿越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。

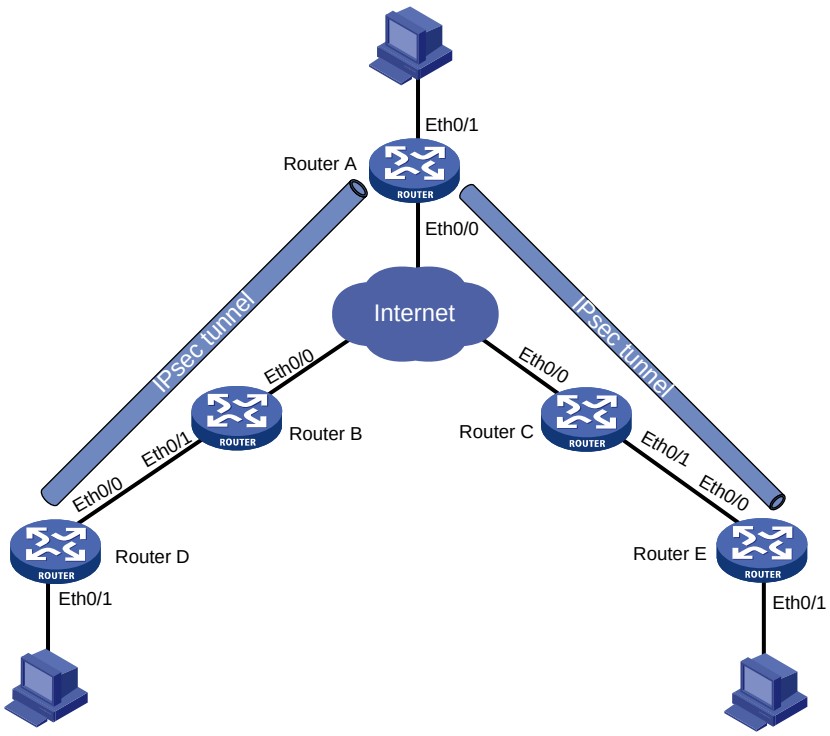
本文档假设您已了解 IPsec 和 NAT 特性。

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 D和Router E是两个分支网关，Router B和Router C 为分支提供 NAT 转换。要求：为了接受协商发起端的访问控制列表设置，Router A 采用安全模板方式分别与 Router D 和 Router E 建立 IPsec VPN，为总部和分支流量进行加密传输。

图1 IPSec VPN 多分支安全模板 NAT 穿越功能的配置举例组网图



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	172.0.0.1/24		Eth0/1	192.168.1.1/24

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	192.168.2.1/24
Router C	Eth0/0	1.0.0.2/24			
	Eth0/1	10.0.2.1/24			

3.2 配置思路

- 为了穿越 NAT，总部与分支之间需要配置成野蛮模式。
- Router A 采用安全模板方式时不需要配置 ACL，接受协商发起端的 ACL。但 Router D 和 Router E 需要配置 ACL，使特定流量匹配安全策略；
- 为了访问总部外网接口，Router D 和 Router E 必须配置静态路由。

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

- 在配置 IPsec 之前，需要保证总部与分支间路由可达。
- 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 172.0.0.1 255.255.255.0
[RouterA-Ethernet0/1] quit
```

配置接口 Ethernet0/0 的 IP 地址。

```
[RouterA] interface ethernet 0/0
[RouterA-Ethernet0/0] ip address 1.0.0.60 255.255.255.0
[RouterA-Ethernet0/0] 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
```

配置到分支内网的静态路由。

```
[RouterA] ip route-static 192.168.1.0 255.255.255.0 1.0.0.1
[RouterA] ip route-static 192.168.2.0 255.255.255.0 1.0.0.2
```

配置本端安全网关的名字为 center。

```
[RouterA] ike local-name center
```

创建一个 IKE 对等体 branch1，并进入 IKE-Peer 视图。

```
[RouterA] ike peer branch1
```

配置 IKE 第一阶段的协商模式为野蛮模式。

```
[RouterA-ike-peer-branch1] exchange-mode aggressive
```

选择 IKE 第一阶段的协商过程中使用 ID 的类型为 name。

```
[RouterA-ike-peer-branch1] id-type name
```

配置对端安全网关的名字。

```
[RouterA-ike-peer-branch1] remote-name branch1
```

配置预共享密钥。

```
[RouterA-ike-peer-branch1] pre-shared-key 123
```

启用 NAT 穿越功能。

```
[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] pre-shared-key 123
[RouterA-ike-peer-branch2] exchange-mode aggressive
[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 Rouer 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 10.0.1.1 255.255.255.0
[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
```

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 Rouer 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 Rouer 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 192.168.1.1 255.255.255.0
[RouterD-Ethernet0/1] 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
```

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 ip source 192.168.1.0 0.0.0.255 destination
 172.0.0.0 0.0.0.255
[RouterD-acl-adv-3000] quit
```

配置本端安全网关的名字为 branch1。

```
[RouterD] ike local-name branch1
```

创建一个 IKE 对等体，并进入 IKE-Peer 视图。

```
[RouterD] ike peer center
```

配置 IKE 第一阶段的协商模式为野蛮模式。

```
[RouterD-ike-peer-center] exchange-mode aggressive
```

配置预共享密钥。

```
[RouterD-ike-peer-center] pre-shared-key 123
```

选择 IKE 第一阶段的协商过程中使用 ID 的类型为 name。

```
[RouterD-ike-peer-center] id-type name
```

配置对端安全网关的名字。

```
[RouterD-ike-peer-center] remote-name center
```

配置远端地址为总部网关的出接口地址。

```
[RouterD-ike-peer-center] remote-address 1.0.0.60
```

启用 NAT 穿越功能。

```
[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 Rouer 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 192.168.2.1 255.255.255.0
[RouterE-Ethernet0/1] 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
```

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 ip source 192.168.2.0 0.0.0.255 destination
 172.0.0.0 0.0.0.255
[RouterE-acl-adv-3000] quit
```

配置本端安全网关的名字为 branch2。

```
[RouterE] ike local-name branch2
```

创建一个 IKE 对等体，并进入 IKE-Peer 视图。

```
[RouterE] ike peer center
```

配置 IKE 第一阶段的协商模式为野蛮模式。

```
[RouterE-ike-peer-center] exchange-mode aggressive
```

配置预共享密钥。

```
[RouterE-ike-peer-center] pre-shared-key 123
```

选择 IKE 第一阶段的协商过程中使用 ID 的类型为 name。

```
[RouterE-ike-peer-center] id-type name
```

配置对端安全网关的名字。

```
[RouterE-ike-peer-center] remote-name center
```

配置远端地址为总部网关的出接口地址。

```
[RouterE-ike-peer-center] remote-address 1.0.0.60
```

启用 NAT 穿越功能。

```
[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，Router A 和 Router D、Router E 可分别实现互通，且数据经 IPsec 进行加密，并不受 NAT 影响。这里以 Router A 与 Router D 为例进行验证。

可以通过如下显示信息看到，Router A 和 Router D 实现互通。

```
<RouterD> ping -a 192.168.1.1 172.0.0.1
  PING 172.0.0.1: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 172.0.0.1: bytes=56 Sequence=1 ttl=255 time=3 ms
    Reply from 172.0.0.1: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 172.0.0.1: bytes=56 Sequence=3 ttl=255 time=3 ms
    Reply from 172.0.0.1: bytes=56 Sequence=4 ttl=255 time=3 ms

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

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: GigabitEthernet0/0
    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: 192.168.1.0/255.255.255.0  port: 0  protocol: IP
        dest addr: 172.0.0.0/255.255.255.0  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 0xA5933FB9(2777890745)
      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): 1843199/3525
      anti-replay detection: Enabled
        anti-replay window size(counter based): 32
      udp encapsulation used for nat traversal: Y

    [outbound ESP SAs]
      spi: 0x30FA0BC7(821693383)
      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): 1843199/3525
      anti-replay detection: Enabled
        anti-replay window size(counter based): 32
      udp encapsulation used for nat traversal: Y
```

3.7 配置文件

- Router A：

```
#
 ike local-name center
#
ike peer branch1
 exchange-mode aggressive
 pre-shared-key cipher $c$3$usDE48gmYI36TbftpJ3+YOBgFaff2w==
 id-type name
 remote-name branch1
 nat traversal
#
ike peer branch2
 exchange-mode aggressive
 pre-shared-key cipher $c$3$vrfgGzDJE8PBS25Mr/tQT7mqCRvraA==
 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 172.0.0.1 255.255.255.0
#
interface Ethernet0/0
 port link-mode route
 ip address 1.0.0.60 255.255.255.0
 ipsec policy branch
#
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 192.168.1.0 255.255.255.0 1.0.0.1
 ip route-static 192.168.2.0 255.255.255.0 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
#
acl number 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 172.0.0.0 0.0.0.255
#
ike peer center
 exchange-mode aggressive
 pre-shared-key cipher $c$3$9ffLIFKA7XqYlM1C5+uvwqH+UJcOEQ==
 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 Ethernet0/0
 port link-mode route
 ip address 10.0.1.2 255.255.255.0
 ipsec policy center
#
interface Ethernet0/1
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 10.0.1.1
#
```

- Router E：

```
#
 ike local-name branch2
#
acl number 3000
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 172.0.0.0 0.0.0.255
#
ike peer center
 exchange-mode aggressive
 pre-shared-key cipher $c$3$9ffLIFKA7XqYlM1C5+uvwqH+UJcOEQ==
 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 Ethernet0/0
 port link-mode route
ip address 10.0.2.2 255.255.255.0
 ipsec policy center
#
interface Ethernet0/1
 port link-mode route
 ip address 192.168.2.1 255.255.255.0
#
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