MSR 系列路由器 ISISv6 over GRE over IPsec 方式穿越 NAT 功能的配置举例

目 录

1 简介

本文档介绍 MSR 系列路由器 ISISv6 over GRE over IPsec 方式穿越 NAT 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、ISIS、IPv6 和 NAT 特性。

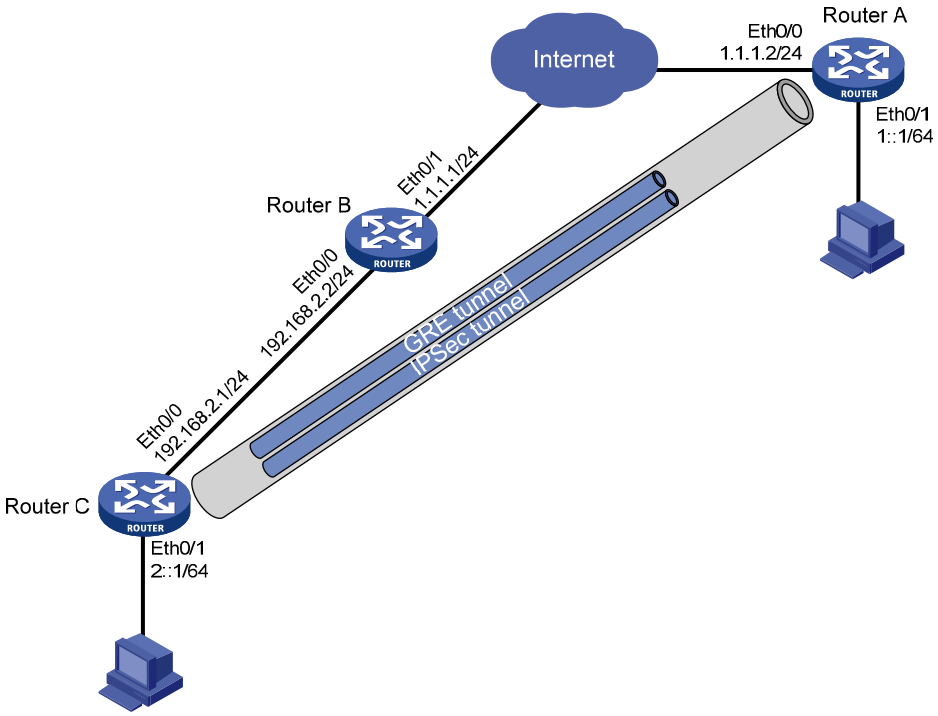
3 配置举例

3.1 组网需求

如 图 1 所示，Router A 和Router C是Ipv6 孤岛的出口网关，Router B是一台NAT设备，要求：

- Router A 和 Router C 建立穿越 NAT 的 IPsec 隧道，对数据流进行加密。
- 在 IPsec 隧道上建立基于 IPv6 的 GRE 隧道。
- 在 GRE 隧道中运行 ISIS 路由协议传递 IPv6 路由，使双方的 IPv6 站点可以互通。

图1 MSR 系列路由器 ISISv6 over GRE over IPsec 方式穿越 NAT 功能的配置组网图



3.2 配置思路

- 为了使 IPsec 穿越 NAT，必须将 IKE 第一阶段协商模式配置为野蛮模式。
- 为了使 ISIS 协议传递 IPv6 路由，GRE 隧道两端和 IPv6 接口必须使能 IS-IS 路由进程的 IPv6 能力。

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

GRE 隧道两端的 IPv6 地址可以手动配置，也可以自动配置链路本地地址。

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 1.1.1.2 255.255.255.0
[RouterA-Ethernet0/0] quit
```

配置接口 Ethernet0/1 的 IPv6 地址。

```
[RouterA] interface ethernet 0/1
[RouterA-Ethernet0/1] ipv6 address 1::1/64
[RouterA-Ethernet0/1] quit
```

配置访问外网的默认路由。

```
[RouterA] ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
```

配置本端安全网关的名字为 rta。

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

全局使能 IPv6。

```
[RouterA] ipv6
```

配置 IKE 对等体。

```
[RouterA] ike peer rtc
[RouterA-ike-peer-rtc] exchange-mode aggressive
[RouterA-ike-peer-rtc] pre-shared-key 123
[RouterA-ike-peer-rtc] id-type name
[RouterA-ike-peer-rtc] remote-name rtc
```

启用 NAT 穿越功能。

```
[RouterA-ike-peer-rtc] nat traversal
[RouterA-ike-peer-rtc] 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 rtc。

```
[RouterA] ipsec policy-template rtc 1
[RouterA-ipsec-policy-template-rtc-1] ike-peer rtc
[RouterA-ipsec-policy-template-rtc-1] proposal def
[RouterA-ipsec-policy-template-rtc-1] quit
```

引用 IPsec 安全策略模板创建一条 IPsec 安全策略。

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

配置路由协议 IPv6 ISIS。

```
[RouterA] isis 1
[RouterA-isis-1] network-entity 11.1111.1111.1111.00
[RouterA-isis-1] ipv6 enable
[RouterA-isis-1] quit
```

配置 GRE 隧道。

```
[RouterA] interface tunnel 0
[RouterA-Tunnel0] ipv6 address auto link-local
[RouterA-Tunnel0] source ethernet 0/0
[RouterA-Tunnel0] destination 192.168.2.1
```

使能 GRE 隧道 IS-IS 路由进程的 IPv6 能力。

```
[RouterA-Tunnel0] isis ipv6 enable 1
[RouterA-Tunnel0] quit
```

在接口 Ethernet0/0 上应用安全策略。

```
[RouterA] interface ethernet 0/0
[RouterA-Ethernet0/0] ipsec policy policy
[RouterA-Ethernet0/0] quit
```

使能接口 IS-IS 路由进程的 IPv6 能力。

```
[RouterA] interface ethernet 0/1
[RouterA-Ethernet0/1] isis ipv6 enable 1
[RouterA-Ethernet0/1] 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 1.1.1.1 255.255.255.0
[RouterB-Ethernet0/1] quit
```

配置接口 Ethernet0/0 的 IP 地址。

```
[RouterB] interface ethernet 0/0
[RouterB-Ethernet0/0] ip address 192.168.2.2 255.255.255.0
[RouterB-Ethernet0/0] quit
```

创建 NAT 转换地址池。

```
[RouterB] nat address-group 0 1.1.1.3 1.1.1.13
```
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 192.168.2.1 0
[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 0/1
[RouterB-Ethernet0/1] nat outbound 2000 address-group 0
[RouterB-Ethernet0/1] 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 192.168.2.1 255.255.255.0
[RouterC-Ethernet0/0] quit
```
配置接口 Ethernet0/1 的 IPv6 地址。
```
[RouterC] interface ethernet 0/1
[RouterC-Ethernet0/1] ipv6 address 2::1/64
[RouterC-Ethernet0/1] quit
```
配置访问外网的默认路由。
```
[RouterC] ip route-static 0.0.0.0 0.0.0.0 192.168.2.2
```
配置本端安全网关的名字为 rtc。
```
[RouterC] ike local-name rtc
```
全局使能 IPv6。
```
[RouterC] ipv6
```
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 gre source 192.168.2.1 0 destination 1.1.1.
2 0
[RouterC-acl-adv-3000] quit
```
配置 IKE 对等体。
```
[RouterC] ike peer rta
[RouterC-ike-peer-rta] exchange-mode aggressive
[RouterC-ike-peer-rta] pre-shared-key 123
[RouterC-ike-peer-rta] id-type name
[RouterC-ike-peer-rta] remote-name rta
[RouterC-ike-peer-rta] remote-address 1.1.1.2
```
启用 NAT 穿越功能。
```
[RouterC-ike-peer-rta] nat traversal
[RouterC-ike-peer-rta] quit
```
采用安全提议的缺省配置。
```
[RouterC] ipsec proposal 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 policy，其协商方式为 isakmp。

```
[RouterC] ipsec policy policy 1 isakmp
[RouterC-ipsec-policy-isakmp-policy-1] security acl 3000
[RouterC-ipsec-policy-isakmp-policy-1] ike-peer rta
[RouterC-ipsec-policy-isakmp-policy-1] proposal def
[RouterC-ipsec-policy-isakmp-policy-1] quit
```

配置路由协议 IPv6 ISIS。

```
[RouterC] isis 1
[RouterC-isis-1] network-entity 22.2222.2222.2222.00
[RouterC-isis-1] ipv6 enable
[RouterC-isis-1] quit
```

配置 GRE 隧道。

```
[RouterC] interface tunnel 0
[RouterC-Tunnel0] ipv6 address auto link-local
[RouterC-Tunnel0] source Ethernet0/0
[RouterC-Tunnel0] destination 1.1.1.2
```

使能 GRE 隧道 IS-IS 路由进程的 IPv6 能力。

```
[RouterC-Tunnel0] isis ipv6 enable 1
[RouterC-Tunnel0] quit
```

在接口 Ethernet0/0 上应用安全策略。

```
[RouterC] interface ethernet 0/0
[RouterC-Ethernet0/0] ipsec policy policy
[RouterC-Ethernet0/0] quit
```

使能接口 IS-IS 路由进程的 IPv6 能力。

```
[RouterC] interface ethernet 0/1
[RouterC-Ethernet0/1] isis ipv6 enable 1
[RouterC-Ethernet0/1] quit
```

3.6 验证配置

完成以上配置后，Router A 和 Router C 之间建立了能使用 ISIS 协议传递 IPv6 路由的 GRE 隧道，且数据经 IPsec 进行加密，并不受 NAT 影响。这里 Router C 为例进行验证。

可以通过如下显示信息看到，Router A 和 Router C 后的 IPv6 孤岛可以实现互通。

```
<RouterC> ping ipv6 -a 2::1 1::1
  PING 1::1 : 56  data bytes, press CTRL_C to break
    Reply from 1::1
    bytes=56 Sequence=0 hop limit=64  time = 3 ms
    Reply from 1::1
    bytes=56 Sequence=1 hop limit=64  time = 9 ms
    Reply from 1::1
    bytes=56 Sequence=2 hop limit=64  time = 3 ms
    Reply from 1::1
```

```
    bytes=56 Sequence=3 hop limit=64  time = 1 ms
    Reply from 1::1
    bytes=56 Sequence=4 hop limit=64  time = 3 ms

  --- 1::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/3/9 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。

```
<RouterC> display ike sa
    total phase-1 SAs:  1
    connection-id  peer                    flag        phase   doi
  ----------------------------------------------------------------
     3             1.1.1.2                 RD|ST       1       IPSEC
     5             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。

```
<RouterC> 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: 192.168.2.1
        remote address: 1.1.1.2
    flow:
        sour addr: 192.168.2.1/255.255.255.255  port: 0  protocol: GRE
        dest addr: 1.1.1.2/255.255.255.255  port: 0  protocol: GRE

    [inbound ESP SAs]
      spi: 0x3D55779D(1029011357)
      transform: ESP-ENCRYPT-NULL ESP-AUTH-MD5
      in use setting: Tunnel
      connection id: 5
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1842990/2462
      anti-replay detection: Enabled
```

```
    anti-replay window size(counter based): 32
  udp encapsulation used for nat traversal: Y

[outbound ESP SAs]
  spi: 0x22E8AAEA(585673450)
  transform: ESP-ENCRYPT-NULL ESP-AUTH-MD5
  in use setting: Tunnel
  connection id: 6
  sa duration (kilobytes/sec): 1843200/3600
  sa remaining duration (kilobytes/sec): 1842991/2462
  anti-replay detection: Enabled
    anti-replay window size(counter based): 32
  udp encapsulation used for nat traversal: Y
```

查看 Router C 的 IPv6 IS-IS 路由表。

```
<RouterC> display isis route ipv6

                      Route information for ISIS(1)
                      -----------------------------

                   ISIS(1) IPv6 Level-1 Forwarding Table
                   -------------------------------------
 Destination: 2::                                  PrefixLen: 64
 Flag       : D/L/-                                Cost     : 10
 Next Hop   : Direct                               Interface: Eth0/0

      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set


                   ISIS(1) IPv6 Level-2 Forwarding Table
                   -------------------------------------
 Destination: 1::                                  PrefixLen: 64
 Flag       : R/-/-                                Cost     : 20
 Next Hop   : FE80::101:102                        Interface: Tun0
              FE80::20F:E2FF:FE3A:FF6B                        Eth0/0

 Destination: 2::                                  PrefixLen: 64
 Flag       : D/L/-                                Cost     : 10
 Next Hop   : Direct                               Interface: Eth0/0

      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

查看 Router C 的 Tunnel 接口状态。

```
<RouterC> display interface tunnel0
Tunnel0 current state: UP
Line protocol current state: UP
Description: Tunnel0 Interface
The Maximum Transmit Unit is 1476
Internet protocol processing : disabled
Encapsulation is TUNNEL, service-loopback-group ID not set.
```

```
Tunnel source 192.168.2.1 (Ethernet0/0), destination 1.1.1.2
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:  177 bytes/sec, 0 packets/sec
    Last 300 seconds output:  177 bytes/sec, 0 packets/sec
    737 packets input,  1039698 bytes
    0 input error
    747 packets output,  1044505 bytes
    0 output error
```

3.7 配置文件

- Router A：

```
#
 ike local-name rta
#
ipv6
#
ike peer rtc
 exchange-mode aggressive
 pre-shared-key cipher $c$3$A3MTEVjp+dMILVyV4Uw0kFcJMYfrJA==
 id-type name
 remote-name rtc
 nat traversal
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy-template rtc 1
 ike-peer rtc
 transform-set def
#
ipsec policy policy 1 isakmp template rtc
#
isis 1
 network-entity 11.1111.1111.1111.00
 #
  ipv6 enable
#
```

```
interface Ethernet0/1
 port link-mode route
 ipv6 address 1::1/64
 isis ipv6 enable 1
interface Ethernet0/0
 port link-mode route
 ip address 1.1.1.2 255.255.255.0
 ipsec policy policy
#
interface Tunnel0
 ipv6 address auto link-local
 source Ethernet0/0
 destination 192.168.2.1
 isis ipv6 enable 1
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
#
```

- Router B：

```
#
 nat address-group 0 1.1.1.3 1.1.1.13
#
acl number 2000
 rule 0 permit source 192.168.2.1 0
#
interface Ethernet0/0
 port link-mode route
 ip address 192.168.2.2 255.255.255.0
#
interface Ethernet0/1
 port link-mode route
 nat outbound 2000 address-group 0
 ip address 1.1.1.1 255.255.255.0
#
```

- Router C：

```
#
 ike local-name rtc
#
ipv6
#
acl number 3000
 rule 0 permit gre source 192.168.2.1 0 destination 1.1.1.2 0
#
ike peer rta
 exchange-mode aggressive
 pre-shared-key cipher $c$3$P1CRcMmHfxHOxGxGEw499ashSB37tQ==
 id-type name
 remote-name rta
 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 rta
 transform-set def
#
isis 1
 network-entity 22.2222.2222.2222.00
 #
  ipv6 enable
#
interface Ethernet0/1
 port link-mode route
 ipv6 address 2::1/64
 isis ipv6 enable 1
#
interface Ethernet0/0
 port link-mode route
 ip address 192.168.2.1 255.255.255.0
 ipsec policy policy
#
interface Tunnel0
 ipv6 address auto link-local
 source Ethernet0/0
 destination 1.1.1.2
 isis ipv6 enable 1
#
 ip route-static 0.0.0.0 0.0.0.0 192.168.2.2
#
```

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