MSR 系列路由器与 SecPath 防火墙实现 GRE 跨越 IPsec VPN 配置举例

目 录

1 简介

本文档介绍 MSR 系列路由器与 SecPath 系列 VPN 接入设备实现 GRE 跨越 IPsec VPN 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 GRE 特性。

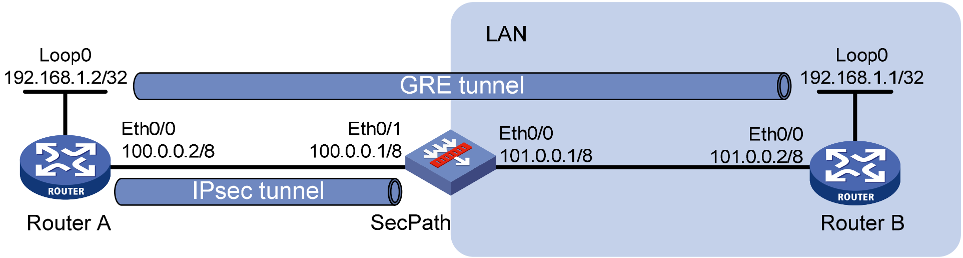
3 配置举例

3.1 组网需求

如 图 1 所示，Router A为某公司分支网关，Router B为总部网关，SecPath为总部的一台防火墙。要求：

- Router A 通过野蛮模式与 SecPath 建立 IPsec VPN，再通过 IPsec VPN 通道与 Router B 建立 GRE 隧道。
- VPN 隧道必须保证在任何一台设备重启的情况下能够自动建立。

图1 MSR 系列路由器与 SecPath 实现 GRE 跨越 IPsec VPN 配置组网图



3.2 配置思路

通过使能 GRE 的 keepalive 功能，探测 Tunnel 接口状态，并配置 keepalive 报文发送周期及最大发送次数来保证任何一台设备重启的情况下能够自动建立 VPN 隧道。

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 VPN 之前需保证各设备间路由可达。

3.5 配置步骤

3.5.1 RouterA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 100.0.0.2 255.0.0.0
[RouterA-Ethernet0/0] quit
```

# 配置用于 GRE 连接的 Loopback 接口地址。

```
[RouterA] interface loopback 0
[RouterA-LoopBack0] ip address 192.168.1.2 255.255.255.255
[RouterA-LoopBack0] quit
```

# 配置 GRE 隧道。

```
[RouterA] interface tunnel 0
[RouterA-Tunnel0] ip address 172.16.1.2 255.255.255.0
[RouterA-Tunnel0] source loopback0
[RouterA-Tunnel0] destination 192.168.1.1
```

# 使能 GRE 的 keepalive 功能，并配置 keepalive 报文发送周期及最大发送次数。

```
[RouterA-Tunnel0] keepalive 3 3
[RouterA-Tunnel0] quit
```

# 配置到总部环回口的静态路由。

```
[RouterA] ip route-static 192.168.1.1 255.255.255.255 100.0.0.1
```

# 配置本端安全网关的名字为 branch。

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

# 配置 IKE 对等体存活检测。

```
[RouterA] ike dpd 1
[RouterA-ike-dpd-1] quit
```

# 创建 ACL3001,定义需要 IPsec 保护的数据流。

```
[RouterA] acl number 3001
[RouterA-acl-adv-3001] rule 0 permit ip source 192.168.1.2 0 destination 192.168.
1.1 0
[RouterA-acl-adv-3001] rule 5 deny ip
[RouterA-acl-adv-3001] quit
```

# 配置 IKE 对等体。

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

```
[RouterA-ike-peer-peer] remote-address 100.0.0.1
[RouterA-ike-peer-peer] nat traversal
[RouterA-ike-peer-peer] dpd 1
[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
[RouterA-ipsec-policy-isakmp-policy-1] security acl 3001
[RouterA-ipsec-policy-isakmp-policy-1] ike-peer peer
[RouterA-ipsec-policy-isakmp-policy-1] proposal def
[RouterA-ipsec-policy-isakmp-policy-1] 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
```

3.5.2 Router B的配置

# 配置接口 Ethernet0/0 的 IP 地址。

```
<RouterB> system-view
[RouterB] interface ethernet 0/0
[RouterB-Ethernet0/0] ip address 101.0.0.2 255.0.0.0
[RouterB-Ethernet0/0] quit
```

# 配置用于 GRE 连接的 Loopback 接口地址。

```
[RouterB] interface loopback 0
[RouterB-LoopBack0] ip address 192.168.1.1 255.255.255.255
[RouterB-LoopBack0] quit
```

# 配置 GRE 隧道。

```
[RouterB] interface tunnel 0
[RouterB-Tunnel0] ip address 172.16.1.1 255.255.255.0
[RouterB-Tunnel0] source loopback0
[RouterB-Tunnel0] destination 192.168.1.2
```

# 使能 GRE 的 keepalive 功能，并配置 keepalive 报文发送周期及最大发送次数。

```
[RouterB-Tunnel0] keepalive 3 3
[RouterB-Tunnel0] quit
```

# 配置到分支环回口的静态路由。

```
[RouterB] ip route-static 192.168.1.2 255.255.255.255 101.0.0.1
```

3.5.3 SecPath的配置

# 配置接口 Ethernet0/0 的 IP 地址。

```
<SecPath> system-view
[SecPath] interface ethernet 0/0
[SecPath-Ethernet0/0] ip address 101.0.0.1 255.0.0.0
[SecPath-Ethernet0/0] quit
```

# 配置接口 Ethernet0/1 的 IP 地址。

```
[SecPath] interface ethernet 0/1
[SecPath-Ethernet0/1] ip address 100.0.0.1 255.0.0.0
[SecPath-Ethernet0/1] quit
```

# 分别配置到总部和分支环回口的静态路由。

```
[SecPath] ip route-static 192.168.1.1 255.255.255.255 101.0.0.2 preference 60
[SecPath] ip route-static 192.168.1.2 255.255.255.255 100.0.0.2 preference 60
```

# 配置安全区域。

```
[SecPath] zone name Trust
[SecPath-zone-Trust] import interface ethernet 0/0
[SecPath-zone-Trust] quit
[SecPath] zone name Untrust
[SecPath-zone-Untrust] import interface ethernet 0/1
[SecPath-zone-Untrust] quit
```

# 配置从 Untrust 区域到 Trust 区域允许所有流量通过。

```
[SecPath] interzone source Untrust destination Trust
[SecPath-interzone-Untrust-Trust] rule permit
[SecPath-interzone-Untrust-Trust-rule-0] source-ip any_address
[SecPath-interzone-Untrust-Trust-rule-0] destination-ip any_address
[SecPath-interzone-Untrust-Trust-rule-0] service any_service
[SecPath-interzone-Untrust-Trust-rule-0] rule enable
[SecPath-interzone-Untrust-Trust-rule-0] quit
```

# 配置本端安全网关的名字为 center。

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

# 配置 IKE 对等体存活检测。

```
[SecPath] ike dpd 1
[SecPath-ike-dpd-1] quit
```

# 配置 IKE 对等体。

```
[SecPath] ike peer peer
[SecPath-ike-peer-peer] exchange-mode aggressive
[SecPath-ike-peer-peer] pre-shared-key 123
[SecPath-ike-peer-peer] id-type name
[SecPath-ike-peer-peer] remote-name branch
[SecPath-ike-peer-peer] nat traversal
[SecPath-ike-peer-peer] dpd 1
[SecPath-ike-peer-peer] quit
```

# 采用安全提议的缺省配置。

```
[SecPath] ipsec proposal def
```

# 配置 ESP 协议采用 md5 认证算法。

```
[SecPath-ipsec-proposal-def] esp authentication-algorithm md5
[SecPath-ipsec-proposal-def] quit
```

# 创建 IPsec 安全策略模板 test。

```
[SecPath] ipsec policy-template test 1
[SecPath-ipsec-policy-template-test-1] ike-peer peer
[SecPath-ipsec-policy-template-test-1] proposal def
[SecPath-ipsec-policy-template-test-1] quit
```

# 引用 IPsec 安全策略模板创建一条 IPsec 安全策略。

```
[SecPath] ipsec policy policy 1 isakmp template test
```

# 在接口 Ethernet0/1 上应用安全策略。

```
[SecPath] interface ethernet 0/1
[SecPath-Ethernet0/1] ipsec policy policy
[SecPath-Ethernet0/1] quit
```

3.6 验证配置

完成以上配置后，Router A 和 Router B 的内网之间可以建立起 GRE over IPsec 隧道。

# 通过以下显示信息，可以看到分支可以访问总部内网。

```
<RouterA> ping -a 192.168.1.2 192.168.1.1
  PING 192.168.1.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.1: bytes=56 Sequence=0 ttl=254 time=4 ms
    Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=254 time=4 ms
    Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=254 time=3 ms
    Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=254 time=3 ms
    Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=254 time=4 ms

  --- 192.168.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/4 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。

```
<RouterA> display ike sa
    total phase-1 SAs:  1
    connection-id  peer                    flag        phase   doi
  ----------------------------------------------------------------
     4             100.0.0.1               RD|ST       1       IPSEC
     5             100.0.0.1               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。

```
<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: 100.0.0.2
        remote address: 100.0.0.1
    flow:
        sour addr: 192.168.1.2/255.255.255.255  port: 0  protocol: IP
        dest addr: 192.168.1.1/255.255.255.255  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 0x1EEC43F8(518800376)
      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): 1843198/3541
      anti-replay detection: Enabled
        anti-replay window size(counter based): 32
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 0xCB1706BE(3407283902)
      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): 1843198/3541
      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。

```
<RouterA>display interface tunnel0
Tunnel0 current state: UP
Line protocol current state: UP
Description: Tunnel0 Interface
The Maximum Transmit Unit is 1476
Internet Address is 172.16.1.2/24 Primary
Encapsulation is TUNNEL, service-loopback-group ID not set.
Tunnel source 192.168.1.2 (LoopBack0), destination 192.168.1.1
Tunnel bandwidth 64 (kbps)
Tunnel keepalive enabled, Period(3 s), Retries(3)
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:  1 bytes/sec, 0 packets/sec
    Last 300 seconds output:  6 bytes/sec, 0 packets/sec
    410 packets input,  4920 bytes
    0 input error
    756 packets output,  18144 bytes
    0 output error
```

3.7 配置文件

- Router A：

```
#
 ike local-name branch
#
acl number 3001
 rule 0 permit ip source 192.168.1.2 0 destination 192.168.1.1 0
 rule 5 deny ip
#
ike dpd 1
#
ike peer peer
 exchange-mode aggressive
 pre-shared-key cipher $c$3$G9fHwlOJSlW7x7fwkULC601R+rHXWg==
 id-type name
 remote-name center
 remote-address 100.0.0.1
 nat traversal
 dpd 1
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy policy 1 isakmp
 security acl 3001
 ike-peer peer
 transform-set def
#
interface Ethernet0/0
 port link-mode route
 ip address 100.0.0.2 255.0.0.0
 ipsec policy policy
#
```

```
interface LoopBack0
 ip address 192.168.1.2 255.255.255.255
#
interface Tunnel0
 ip address 172.16.1.2 255.255.255.0
 source LoopBack0
 destination 192.168.1.1
 keepalive 3 3
#
 ip route-static 192.168.1.1 255.255.255.255 100.0.0.1
#
```

- Router B：

```
#
interface Ethernet0/0
 port link-mode route
 ip address 101.0.0.2 255.0.0.0
#
interface LoopBack0
 ip address 192.168.1.1 255.255.255.255
#
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 source LoopBack0
 destination 192.168.1.2
 keepalive 3 3
#
 ip route-static 192.168.1.2 255.255.255.255 101.0.0.1
#
```

- SecPath：

```
#
zone name Trust id 2
 priority 85
 import interface Ethernet0/0
zone name Untrust id 4
 priority 5
 import interface Ethernet0/1
interzone source Untrust destination Trust
  rule 0 permit
  source-ip any_address
  destination-ip any_address
  service any_service
  rule enable
#
 ike local-name center
#
acl number 3000
 rule 0 permit gre source 192.168.1.2 0 destination 192.168.1.1 0
#
```

```
ike dpd 1
#
ike peer peer
 exchange-mode aggressive
 pre-shared-key cipher TEzJOUGCmuE=
 id-type name
 remote-name branch
 nat traversal
 dpd 1
#
ipsec proposal def
#
ipsec policy-template test 1
 ike-peer peer
 proposal def
#
ipsec policy policy 1 isakmp template test
#
interface Ethernet0/0
 port link-mode route
 ip address 101.0.0.1 255.0.0.0
#
interface Ethernet0/1
 port link-mode route
 ip address 100.0.0.1 255.0.0.0
 ipsec policy policy
#
ip route-static 192.168.1.1 255.255.255.255 101.0.0.2
ip route-static 192.168.1.2 255.255.255.255 100.0.0.2
#
```

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