

MSR 系列路由器 GRE over IPsec 典型配置举例

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 配置注意事项	2
3.5 配置步骤	2
3.5.1 RouterA的配置	2
3.5.2 RouterB的配置	3
3.6 验证配置	4
3.7 配置文件	5
4 相关资料	6

1 简介

本文档介绍 GRE over IPsec 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。

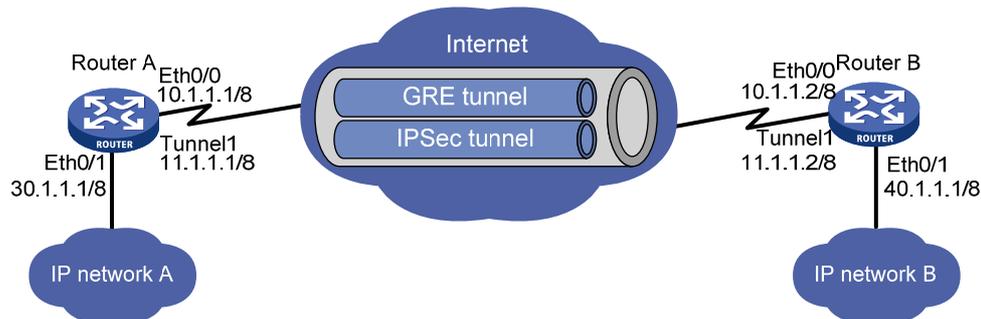
本文档假设您已了解 GRE 和 IPsec 特性。

3 配置举例

3.1 组网需求

如 [图 1](#) 所示，IP network A 的接入路由器采用 Router A，IP network B 的接入路由器采用 Router B，采用 GRE 技术通过 VPN 相连。要求：为进一步保障两公司之间的数据机密性，需要在现有 VPN 的基础上，启用 IPsec 对数据进行加密保护。

图1 GRE over IPsec 配置组网图



3.2 配置思路

- 通过配置静态路由穿越 GRE 隧道，从而使两端私网之间可以互通。
- 将 IPsec 与 GRE 结合使用，可以对通过 GRE 隧道的路由即两端私网间的通信进行保护。
- 将 ACL 中源、目的 IP 地址与建立 GRE 隧道的源、目的 IP 地址配置相同，可以对整个 GRE 隧道进行保护

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

由于 GRE over IPsec 将对 GRE 封装后的数据进行 IPsec 封装，因此在配置访问控制列表时，需要匹配经 GRE 封装后的数据流。

3.5 配置步骤

3.5.1 RouterA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 30.1.1.1 8
[RouterA-Ethernet0/1] quit
```

配置 GRE 隧道。

```
[RouterA] interface tunnel 1
[RouterA-Tunnel1] ip address 11.1.1.1 8
[RouterA-Tunnel1] source 10.1.1.1
[RouterA-Tunnel1] destination 10.1.1.2
[RouterA-Tunnel1] quit
```

配置静态路由。

```
[RouterA] ip route-static 40.0.0.0 255.0.0.0 Tunnel1
```

创建 ACL3000，定义需要 IPsec 保护的数据流。

```
[RouterA] acl number 3000
[RouterA-acl-adv-3000] rule permit ip source 10.1.1.1 0.0.0.0 destination 10.1.1.2 0.0.0.0
[RouterA-acl-adv-3000] rule deny ip source any destination any
[RouterA-acl-adv-3000] quit
```

创建 IKE 对等体。

```
[RouterA] ike peer test
[RouterA-ike-peer-test] pre-shared-key test
[RouterA-ike-peer-test] remote-address 10.1.1.2
[RouterA-ike-peer-test] quit
```

创建 IPsec 安全提议。

```
[RouterA] ipsec proposal test
[RouterA-ipsec-proposal-test] encapsulation-mode tunnel
[RouterA-ipsec-proposal-test] transform esp
[RouterA-ipsec-proposal-test] esp encryption-algorithm 3des
[RouterA-ipsec-proposal-test] esp authentication-algorithm sha
[RouterA-ipsec-proposal-test] quit
```

创建 IPsec 安全策略。

```
[RouterA] ipsec policy test 1 isakmp
[RouterA-ipsec-policy-isakmp-test-1] security acl 3000
[RouterA-ipsec-policy-isakmp-test-1] ike-peer test
[RouterA-ipsec-policy-isakmp-test-1] proposal test
[RouterA-ipsec-policy-isakmp-test-1] quit
```

在接口 Ethernet0/0 上应用 IPsec 安全策略。

```
[RouterA] interface ethernet 0/0
[RouterA-Ethernet0/0] ipsec policy test
[RouterA-Ethernet0/0] ip address 10.1.1.1 8
[RouterA-Ethernet0/0] quit
```

3.5.2 RouterB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 40.1.1.1 8
[RouterB-Ethernet0/1] quit
```

配置 GRE 隧道。

```
[RouterB] interface tunnel 1
[RouterB-Tunnel1] ip address 11.1.1.2 8
[RouterB-Tunnel1] source 10.1.1.2
[RouterB-Tunnel1] destination 10.1.1.1
[RouterB-Tunnel1] quit
```

配置静态路由。

```
[RouterB] ip route-static 30.0.0.0 255.0.0.0 Tunnel1
```

创建 ACL3000，定义需要 IPsec 保护的数据流。

```
[RouterB] acl number 3000
[RouterB-acl-adv-3000] rule permit ip source 10.1.1.2 0.0.0.0 destination 10.1.1.1 0.0.0.0
[RouterB-acl-adv-3000] rule deny ip source any destination any
[RouterB-acl-adv-3000] quit
```

创建 IKE 对等体。

```
[RouterB] ike peer test
[RouterB-ike-peer-test] pre-shared-key test
[RouterB-ike-peer-test] remote-address 10.1.1.1
[RouterB-ike-peer-test] quit
```

创建 IPsec 安全提议。

```
[RouterB] ipsec proposal test
[RouterB-ipsec-proposal-test] encapsulation-mode tunnel
[RouterB-ipsec-proposal-test] transform esp
[RouterB-ipsec-proposal-test] esp encryption-algorithm 3des
[RouterB-ipsec-proposal-test] esp authentication-algorithm sha
[RouterB-ipsec-proposal-test] quit.
```

创建 IPsec 安全策略。

```
[RouterB] ipsec policy test 1 isakmp
[RouterB-ipsec-policy-isakmp-test-1] security acl 3000
[RouterB-ipsec-policy-isakmp-test-1] ike-peer test
[RouterB-ipsec-policy-isakmp-test-1] proposal test
[RouterB-ipsec-policy-isakmp-test-1] quit
```

在接口 Ethernet0/0 上应用 IPsec 安全策略。

```
[RouterB] interface ethernet 0/0
[RouterB-Ethernet0/0] ipsec policy test
[RouterB-Ethernet0/0] ip address 10.1.1.2 8
[RouterB-Ethernet0/0] quit
```

3.6 验证配置

(1) 查看 IKE SA

配置完成后从 30.1.1.1 ping 40.1.1.1, 会触发 IPsec 协商, 建立 IPsec 隧道。在成功建立 IPsec 隧道后, 可以 ping 通。在系统视图下使用 **display ike sa** 命令, 可以看到两个阶段的 SA 正常建立, 以 Router A 为例:

```
[RouterA] display ike sa
total phase-1 SAs: 1
connection-id peer flag phase doi
-----
1 10.1.1.2 RD|ST 1 IPSEC
2 10.1.1.2 RD|ST 2 IPSEC
flag meaning
RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
```

(2) 查看 ipsec sa

在系统视图下使用 **display ipsec sa** 命令可以看到 ipsec sa 的建立情况。以 Router A 为例:

```
[RouterA] display ipsec sa
=====
Interface: Ethernet0/0
path MTU: 1500
=====

-----
IPsec policy name: "test"
sequence number: 1
mode: isakmp
-----

connection id: 1
encapsulation mode: tunnel
perfect forward secrecy:
tunnel:
local address: 10.1.1.1
remote address: 10.1.1.2
flow:
sour addr: 10.1.1.1/255.255.255.255 port: 0 protocol: IP
dest addr: 10.1.1.2/255.255.255.255 port: 0 protocol: IP

[inbound ESP SAs]
spi: 1149793347 (0x44887443)
proposal: ESP-ENCRYPT-3DES ESP-AUTH-SHA1
sa duration (kilobytes/sec): 1843200/3600
sa remaining duration (kilobytes/sec): 1843199/3471
```

```

max received sequence-number: 5
anti-replay check enable: Y
anti-replay window size: 32
udp encapsulation used for nat traversal: N

[outbound ESP SAs]
spi: 2381952527 (0x8df9b60f)
proposal: ESP-ENCRYPT-3DES ESP-AUTH-SHA1
sa duration (kilobytes/sec): 1843200/3600
sa remaining duration (kilobytes/sec): 1843198/3471
max received sequence-number: 12
udp encapsulation used for nat traversal: N

```

3.7 配置文件

- Router A:

```

#
acl number 3000
 rule 0 permit ip source 10.1.1.1 0 destination 10.1.1.2 0
 rule 5 deny ip
#
ike peer test
 pre-shared-key cipher pTHDptKNjg0=
 remote-address 10.1.1.2
#
ipsec proposal test
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy test 1 isakmp
 security acl 3000
 ike-peer test
 proposal test
#
interface Ethernet0/0
 port link-mode route
 ip address 10.1.1.1 255.0.0.0
 ipsec policy test
#
interface Ethernet0/1
 port link-mode route
 ip address 30.1.1.1 255.0.0.0
#
interface Tunnell
 ip address 11.1.1.1 255.0.0.0
 source 10.1.1.1
 destination 10.1.1.2
#

```

```

ip route-static 40.0.0.0 255.0.0.0 Tunnel1
#
● Router B:
#
acl number 3000
  rule 0 permit ip source 10.1.1.2 0 destination 10.1.1.1 0
  rule 5 deny ip
#
ike peer test
  pre-shared-key cipher pTHDptKNjg0=
  remote-address 10.1.1.1
#
ipsec proposal test
  esp authentication-algorithm sha1
  esp encryption-algorithm 3des
#
ipsec policy test 1 isakmp
  security acl 3000
  ike-peer test
  proposal test
#
interface Ethernet0/0
  port link-mode route
  ip address 10.1.1.2 255.0.0.0
  ipsec policy test
#
interface Ethernet0/1
  port link-mode route
  ip address 40.1.1.1 255.0.0.0
#
interface Tunnel1
  ip address 11.1.1.2 255.0.0.0
  source 10.1.1.2
  destination 10.1.1.1
#
ip route-static 30.0.0.0 255.0.0.0 Tunnel1
#

```

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