MSR 系列路由器 IPsec over GRE 典型配置举例

目 录

1 简介

本文档介绍 IPsec over GRE 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。

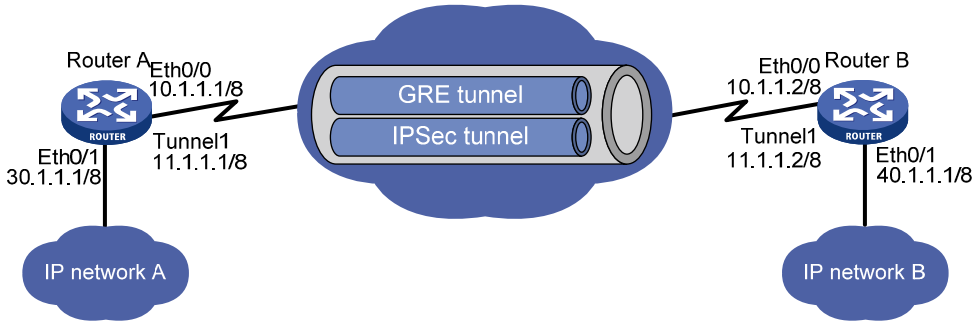
3 配置举例

3.1 组网需求

如 图 1 所示，IP network A的接入路由器为RouterA，IP network B的接入路由器为RouterB，要求：

- Router A 和 Router B 之间建立 GRE 隧道，实现内网之间的互通。
- 在 GRE 隧道上建立 IPsec 隧道，对部分流量进行加密。

图1 IPsec over GRE 的配置组网图



3.2 配置思路

- 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。
- 通过 ACL 指定具体需要保护的数据流，并将 IPsec 应用在 GRE 接口下，可以只对指定的数据流进行保护，其它穿越 GRE 隧道而未指定的数据流不在保护范围之内。

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

- 要将所有的 IPsec 策略都绑定在对应的 GRE 接口上；
- 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 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 10.1.1.1 8
[RouterA-Ethernet0/0] quit
```

配置接口 Ethernet0/1 的 IP 地址。

```
[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 30.0.0.0 0.255.255.255 destination 40.0.0.0
0.255.255.255
[RouterA-acl-adv-3000] quit
```

配置 IKE 对等体。

```
[RouterA] ike peer test
[RouterA-ike-peer-test] pre-shared-key test
[RouterA-ike-peer-test] remote-address 11.1.1.2
[RouterA-ike-peer-test] quit
```

配置 IPsec 安全提议。

```
[RouterA] ipsec proposal test
[RouterA-ipsec-proposal-test] transform esp
[RouterA-ipsec-proposal-test] esp encryption-algorithm 3des
[RouterA-ipsec-proposal-test] esp authentication-algorithm sha1
[RouterA-ipsec-proposal-test] encapsulation-mode tunnel
[RouterA-ipsec-proposal-test] quit
```

配置 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 GRE 隧道接口应用 IPsec 安全策略。

```
[RouterA] interface tunnel 1
[RouterA-Tunnel1] ipsec policy test
[RouterA-Tunnel1] quit
```

3.5.2 RouterB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 10.1.1.2 8
[RouterB-Ethernet0/0] quit
```

配置接口 Ethernet0/1 的 IP 地址。

```
[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 40.0.0.0 0.255.255.255 destination  30.0.0.0
0.255.255.255
[RouterB-acl-adv-3000] quit
```

配置 IKE 对等体。

```
[RouterB] ike peer test
[RouterB-ike-peer-test] pre-shared-key test
[RouterB-ike-peer-test] remote-address 11.1.1.1
[RouterB-ike-peer-test] quit
```

配置 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
```

配置 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 GRE 隧道接口应用 IPsec 安全策略。

```
[RouterB] interface tunnel 1
[RouterB-Tunnel1] ipsec policy test
[RouterB-Tunnel1] quit
```

3.6 验证配置

以 Router B 为例：

配置完成后从 40.1.1.1 ping 30.1.1.1，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。

```
[RouterB] display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  ----------------------------------------------------------
        3          11.1.1.1        RD|ST         1     IPSEC
        4          11.1.1.1        RD|ST         2     IPSEC
  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
 [RouterB]
```

在系统视图下使用 **display ipsec sa** 命令可以看到 IPsec sa 的建立情况。

```
[RouterB] display ipsec sa
==============================
Interface: Tunnel1
    path MTU: 64000
==============================
  ----------------------------
  IPsec policy name: "test 1"
  sequence number: 1
  mode: isakmp
  ----------------------------
    connection id: 3
    encapsulation mode: tunnel
    perfect forward secrecy: None
    tunnel:
        local  address: 11.1.1.2
        remote address: 11.1.1.1
    flow:    (8 times matched)
        sour addr: 40.0.0.0/255.0.0.0  port: 0  protocol: IP
        dest addr: 30.0.0.0/255.0.0.0  port: 0  protocol: IP
    [inbound ESP SAs]
      spi: 421674642 (0x19223e92)
      proposal: ESP-ENCRYPT-3DES ESP-AUTH-SHA1
```

```
    sa remaining key duration (bytes/sec): 1887436464/3396
    max received sequence-number: 4
    udp encapsulation used for nat traversal: N
  [outbound ESP SAs]
    spi: 2489827276 (0x9467bfcc)
    proposal: ESP-ENCRYPT-3DES ESP-AUTH-SHA1
    sa remaining key duration (bytes/sec): 1887436464/3396
    max sent sequence-number: 5
    udp encapsulation used for nat traversal: N
```

在系统视图下使用 **display ipsec tunnel** 命令可以看到隧道的统计信息。

```
[RouterB] display ipsec tunnel
  -----------------------------------------------
  Connection ID : 3
  Perfect forward secrecy: None
  SA's SPI :
      Inbound :  421674642 (0x19223e92) [ESP]
      Outbound : 2489827276 (0x9467bfcc) [ESP]
  Tunnel :
      Local Address:  11.1.1.2  Remote Address : 11.1.1.1
  Flow :     (8 times matched)
      Sour Addr : 40.0.0.0/255.0.0.0  Port: 0  Protocol : IP
      Dest Addr : 30.0.0.0/255.0.0.0  Port: 0  Protocol : IP
  Current Encrypt-card : None
```

3.7 配置文件

- Router A：

```
#
acl number 3000
 rule 0 permit ip source 30.0.0.0 0.255.255.255 destination 40.0.0.0 0.255.255.2
55
#
ike peer test
 pre-shared-key cipher pTHDptKNjg0=
 remote-address 11.1.1.2
#
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
```

```
#
interface Ethernet0/1
 port link-mode route
 ip address 30.1.1.1 255.0.0.0
#
interface Tunnel1
 ip address 11.1.1.1 255.0.0.0
 source 10.1.1.1
 destination 10.1.1.2
 ipsec policy test
#
ip route-static 40.0.0.0 255.0.0.0 Tunnel1
#
```

- Router B：

```
#
acl number 3000
 rule 0 permit ip source 40.0.0.0 0.255.255.255 destination 30.0.0.0 0.255.255.2
55
#
ike peer test
 pre-shared-key cipher pTHDptKNjg0=
 remote-address 11.1.1.1
#
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
#
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
 ipsec policy test
#
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