MSR 系列路由器 GRE over IPsec with OSPF 典型配置举例

目 录

1 简介

本文档介绍 GRE over IPsec with OSPF 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、GRE 和 OSPF 特性。

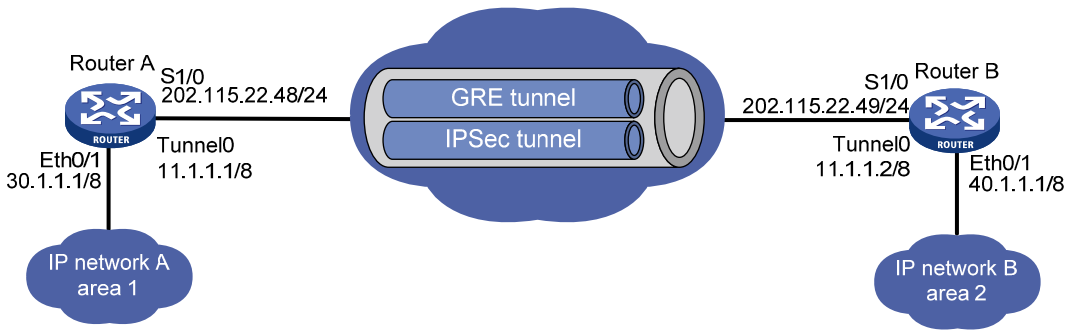
3 配置举例

3.1 组网需求

如 图 1 所示，Router A和Router B是某公司位于不同地点的两个网络的网关，要求：

- 建立 GRE 隧道使内网之间可以互通。
- 在 GRE 隧道上运行 OSPF，传递内网路由。
- 建立 IPsec 隧道，对 OSPF 的路由信息进行加密，使它安全的穿越外部网络，而不会泄漏内部网络的路由。

图1 GRE over IPsec with OSPF 配置组网图



3.2 配置思路

- 将 GRE 隧道与 OSPF 结合使用，可以通过 GRE 来传递 OSPF 路由，从而使企业私网之间可以互通。
- 将 IPsec 与 GRE 结合使用，可以对通过 GRE 隧道的路由即企业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 2207 版本上进行配置和验证的。

3.4 配置注意事项

不能将建立 GRE 隧道连接的接口加入到 OSPF，否则连接会失效。

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 30.1.1.1 255.0.0.0
[RouterA-Ethernet0/1] quit
```

配置接口 serial 1/0 的 IP 地址。

```
[RouterA] interface serial 1/0
[RouterA-Serial1/0] link-protocol ppp
[RouterA-Serial1/0 ]ip address 202.115.22.48 255.255.255.0
[RouterA-Serial1/0] quit
```

创建 ACL3000,定义需要 IPsec 保护的数据流。

```
[RouterA] acl number 3000
[RouterA-acl-adv-3000] rule 0 permit ip source 202.115.22.48 0 destination 202.115.22.49 0
[RouterA-acl-adv-3000] quit
```

配置 IKE 对等体。

```
[RouterA] ike peer test
[RouterA-ike-peer-test] pre-shared-key 123
[RouterA-ike-peer-test] remote-address 202.115.22.49
[RouterA-ike-peer-test] quit
```

配置 IPsec 安全提议。

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

配置 IPsec 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 serial 1/0 上应用 IPsec 策略。

```
[RouterA] interface serial 1/0
[RouterA-Serial1/0] ipsec policy test
```

```
[RouterA-Serial1/0] quit
```
配置 GRE 隧道。
```
[RouterA] interface tunnel 0
[RouterA-Tunnel0] ip address 11.1.1.1 255.0.0.0
[RouterA-Tunnel0] source 202.115.22.48
[RouterA-Tunnel0] destination 202.115.22.49
[RouterA-Tunnel0] gre key 4533
[RouterA-Tunnel0] gre checksum
[RouterA-Tunnel0] quit
```
配置 OSPF 路由协议。
```
[RouterA] ospf 1
[RouterA-ospf-1] area 0.0.0.0
[RouterA-ospf-1-area-0.0.0.0] network 11.0.0.0 0.255.255.255
[RouterA-ospf-1-area-0.0.0.0] area 0.0.0.1
[RouterA-ospf-1-area-0.0.0.1] network 30.0.0.0 0.255.255.255
[RouterA-ospf-1-area-0.0.0.1] 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 40.1.1.1 255.0.0.0
[RouterB-Ethernet0/1] quit
```
配置接口 serial 1/0 的 IP 地址。
```
[RouterB] interface serial 1/0
[RouterB-Serial1/0] link-protocol ppp
[RouterB-Serial1/0] ip address 202.115.22.49 255.255.255.0
[RouterB-Serial1/0] quit
```
创建 ACL3000,定义需要 IPsec 保护的数据流。
```
[RouterB] acl number 3000
[RouterB-acl-adv-3000] rule 0 permit ip source 202.115.22.49 0 destination 202.115.22.48 0
[RouterB-acl-adv-3000] quit
```
配置 IKE 对等体。
```
[RouterB]ike peer test
[RouterB-ike-peer-test] pre-shared-key 123
[RouterB-ike-peer-test] remote-address 202.115.22.48
[RouterB-ike-peer-test] quit
```
配置 IPsec 安全提议。
```
[RouterB] ipsec proposal test
[RouterB-ipsec-proposal-test] esp authentication-algorithm sha1
[RouterB-ipsec-proposal-test] esp encryption-algorithm 3des
[RouterB-ipsec-proposal-test] quit
```
配置 IPsec 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 serial 1/0 上应用 IPsec 策略。

```
[RouterB] interface serial 1/0
[RouterB-Serial1/0] ipsec policy test
[RouterB-Serial1/0] quit
```

配置 GRE 隧道。

```
[RouterB] interface tunnel 0
[RouterB-Tunnel0] ip address 11.1.1.2 255.0.0.0
[RouterB-Tunnel0] source 202.115.22.49
[RouterB-Tunnel0] destination 202.115.22.48
[RouterB-Tunnel0] gre key 4533
[RouterB-Tunnel0] gre checksum
[RouterB-Tunnel0] quit
```

配置 OSPF 路由协议。

```
[RouterB] ospf 1
[RouterB-ospf-1] area 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 11.0.0.0 0.255.255.255
[RouterB-ospf-1-area-0.0.0.0] area 0.0.0.2
[RouterB-ospf-1-area-0.0.0.2] network 40.0.0.0 0.255.255.255
[RouterB-ospf-1-area-0.0.0.2] quit
```

3.6 验证配置

配置完成后 OSPF 通过 GRE 的 tunnel 接口向外发送 hello 报文，由于 hello 报文经过 GRE 封装，匹配了 acl 规则，因此触发了 ike 协商。在 OSPF 建立邻居关系的同时，IPsec 经过协商后也会建立起 IPsec 隧道。以 Router A 为例，使用 **display ike sa** 命令可以查看 sa 建立情况。

```
<RouterA> display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  ----------------------------------------------------------------
     8             202.115.22.49   RD|ST         1     IPSEC
     9             202.115.22.49   RD|ST         2     IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
```

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

```
<RouterA> display ipsec sa
==============================
Interface: Serial1/0
    path MTU: 1500
==============================

  ----------------------------
  IPsec policy name: "test"
```

```
  sequence number: 1
  mode: isakmp
  -----------------------------
    connection id: 1
    encapsulation mode: tunnel
    perfect forward secrecy:
    tunnel:
        local  address: 202.115.22.48
        remote address: 202.115.22.49
    flow:
        sour addr: 202.115.22.48/255.255.255.255  port: 0  protocol: IP
        dest addr: 202.115.22.49/255.255.255.255  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 54798862 (0x3442a0e)
      proposal: ESP-ENCRYPT-3DES ESP-AUTH-SHA1
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843197/3390
      max received sequence-number: 25
      anti-replay check enable: Y
      anti-replay window size: 32
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 2040435079 (0x799e9187)
      proposal: ESP-ENCRYPT-3DES ESP-AUTH-SHA1
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843196/3390
      max received sequence-number: 31
      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。

```
<RouterA> display ipsec tunnel
    total tunnel : 1
    -----------------------------------------------
    connection id: 1
    perfect forward secrecy:
    SA's SPI:
        inbound:  54798862 (0x3442a0e) [ESP]
        outbound: 2040435079 (0x799e9187) [ESP]
    tunnel:
        local  address: 202.115.22.48
        remote address: 202.115.22.49
    flow:
        sour addr: 202.115.22.48/255.255.255.255  port: 0  protocol: IP
        dest addr: 202.115.22.49/255.255.255.255  port: 0  protocol: IP
    current Encrypt-card:
```

3.7 配置文件

- Router A：

```
#
acl number 3000
 rule 0 permit ip source 202.115.22.48 0 destination 202.115.22.49 0
#
ike peer test
 pre-shared-key cipher pTHDptKNjg0=
 remote-address 202.115.22.49
#
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 Ethernet0/1
 port link-mode route
ip address 30.1.1.1 255.0.0.0
#
interface Serial1/0
 link-protocol ppp
 ip address 202.115.22.48 255.255.255.0
 ipsec policy test
#
interface Tunnel0
 ip address 11.1.1.1 255.0.0.0
 source 202.115.22.48
 destination 202.115.22.49
 gre key 4533
 gre checksum
#
ospf 1
 area 0.0.0.0
  network 11.0.0.0 0.255.255.255
 area 0.0.0.1
  network 30.0.0.0 0.255.255.255
#
```

- Router B：

```
#
acl number 3000
 rule 0 permit ip source 202.115.22.49 0 destination 202.115.22.48 0
#
```

```
ike peer test
 pre-shared-key cipher pTHDptKNjg0=
 remote-address 202.115.22.48
#
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 Ethernet0/1
 port link-mode route
ip address 40.1.1.1 255.0.0.0
#
interface Serial1/0
 port link-protocol ppp
ip address 202.115.22.49 255.255.255.0
 ipsec policy test
#
interface Tunnel0
 ip address 11.1.1.2 255.0.0.0
 source 202.115.22.49
 destination 202.115.22.48
 gre key 4533
 gre checksum
#
ospf 1
 area 0.0.0.0
  network 11.0.0.0 0.255.255.255
 area 0.0.0.2
  network 40.0.0.0 0.255.255.255
#
```

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