MSR系列路由器双链路备份环境中IPsec应用方案的配置举例

目 录

1 简介

本文档介绍双链路备份环境中 IPsec 应用方案的典型配置举例。

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。

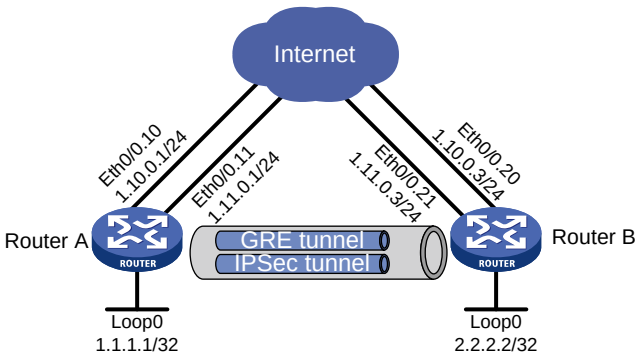
本文档假设您已了解 GRE、IPsec 和 VLAN 终结特性。

3 配置举例

3.1 组网需求

如 图 1 所示，Router A和Router B各有两条链路连接到互连网，可以实现主备链路的切换，提高应用的可靠性。出于安全的考虑，要求对Router A和Router B之间私网数据进行IPsec加密。

图1 双链路备份环境中 IPsec 应用方案的配置组网图



3.2 配置思路

- 由于在一个发起方的 IKE Peer 中，只能和一个 remote-address 发起协商，把 IPsec 策略下发到物理接口时，只能建立 2 对 SA，没有办法建立 4 对；而且，当 Router A 主备接口和 Router B 主备接口同时 Down，那么此时 IPsec SA 将无法使用，客户内网流量将被中断。因此，可以建立一个 GRE 虚接口，然后把 IPsec 策略下发到 GRE 隧道中，IPsec SA 可以保证和 GRE 接口同时存活，再把私网数据导入到 GRE 隧道中即可实现加密。
- Router A 和 Router B 的内网中的 VLAN 各不相同，为了实现指定 VLAN 间的互通，需要使用 VLAN 终结功能。

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

- 注意要把 IPsec 加密和链路备份分开实现，通过 GRE 隧道屏蔽传输链路的切换，为 IPsec SA 建立一个始终 UP 的接口，最终做到网络切换，SA 不切换。
- 注意把 GRE 的源、目的地址路由引入到 Internet 中，并且要求 Internet 可以根据主备链路状况进行路由切换。

3.5 配置步骤

3.5.1 Router A的配置

创建环回接口 Loopback0。

```
<RouterA> system-view
[RouterA] interface loopback 0
[RouterA-LoopBack0] ip address 1.1.1.1 255.255.255.255
[RouterA-LoopBack0] quit
```

配置主链路子接口 IP 地址。

```
[RouterA] interface ethernet 0/0.10
[RouterA-Ethernet0/0.10] ip address 1.10.0.1 255.255.255.0
```

使能 Dot1q 终结功能，并指定可以终结的最外层 VLAN ID 为 10 的报文。

```
[RouterA-Ethernet0/0.10] vlan-type dot1q vid 10
[RouterA-Ethernet0/0.10] quit
```

配置备份链路子接口 IP 地址。

```
[RouterA] interface ethernet 0/0.11
[RouterA-Ethernet0/0.11] ip address 1.11.0.1 255.255.255.0
```

使能 Dot1q 终结功能，并指定可以终结的最外层 VLAN ID 为 11 的报文。

```
[RouterA-Ethernet0/0.11] vlan-type dot1q vid 11
[RouterA-Ethernet0/0.11] quit
```

创建内网接口。

```
[RouterA] interface vlan-interface1
[RouterA-Vlan-interface1] ip address 192.168.1.1 255.255.255.0
[RouterA-Vlan-interface1] quit
```

配置 GRE 隧道，以环回口地址做为隧道源和目的地址。

```
[RouterA] interface tunnel 0
[RouterA-Tunnel0] ip address 1.2.0.1 255.255.255.252
[RouterA-Tunnel0] source loopback0
[RouterA-Tunnel0] destination 2.2.2.2
[RouterA-Tunnel0] quit
```

配置到 Router B 的环回口的静态路由，下一跳指向外网，并设置主备链路。

```
[RouterA] ip route-static 2.2.2.2 255.255.255.255 1.10.0.2
```

```
[RouterA] ip route-static 2.2.2.2 255.255.255.255 1.11.0.2 preference 100
```
配置到 Router B 内网的静态路由，下一跳为对端 GRE 隧道接口地址。
```
[RouterA] ip route-static 192.168.2.0 255.255.255.0 1.2.0.2
```
配置 ACL，定义由 192.168.1.0/24 到 192.168.2.0/24 的数据流。
```
[RouterA] acl number 3000
[RouterA-acl-adv-3000] rule 0 permit ip source 192.168.1.0 0.0.0.255 destination
 192.168.2.0 0.0.0.255
[RouterA-acl-adv-3000] quit
```
配置 IKE 对等体。
```
[RouterA-acl-adv-3000] ike peer peer
[RouterA-ike-peer-peer] pre-shared-key 123
[RouterA-ike-peer-peer] remote-address 1.2.0.2
[RouterA-ike-peer-peer] quit
```
采用安全提议的缺省配置。
```
[RouterA] ipsec proposal def
[RouterA-ipsec-transform-set-def] esp authentication-algorithm md5
[RouterA-ipsec-transform-set-def] quit
```
配置 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 3000
[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 GRE 隧道接口上应用安全策略。
```
[RouterA] interface tunnel 0
[RouterA-Tunnel0] ipsec policy policy
[RouterA-Tunnel0] quit
```

3.5.2 Router B的配置

创建环回接口 Loopback0。
```
<RouterB> system-view
[RouterB] interface loopback 0
[RouterB-LoopBack0] ip address 2.2.2.2 255.255.255.255
[RouterB-LoopBack0] quit
```
配置主链路子接口 IP 地址。
```
[RouterB] interface ethernet 0/0.20
[RouterB-Ethernet0/0.20] ip address 1.10.0.3 255.255.255.0
```
使能 Dot1q 终结功能，并指定可以终结的最外层 VLAN ID 为 20 的报文。
```
[RouterB-Ethernet0/0.20] vlan-type dot1q vid 20
[RouterB-Ethernet0/0.20] quit
```
配置备份链路子接口 IP 地址。
```
[RouterB] interface ethernet 0/0.21
[RouterB-Ethernet0/0.21] ip address 1.11.0.3 255.255.255.0
```
使能 Dot1q 终结功能，并指定可以终结的最外层 VLAN ID 为 21 的报文。

```
[RouterB-Ethernet0/0.21] vlan-type dot1q vid 21
[RouterB-Ethernet0/0.21] quit
```
创建内网接口。
```
[RouterB] interface vlan-interface1
[RouterB-Vlan-interface1] ip address 192.168.2.1 255.255.255.0
[RouterB-Vlan-interface1] quit
```
配置 GRE 隧道，以环回口地址做为隧道源和目的地址。
```
[RouterB] interface tunnel 0
[RouterB-Tunnel0] ip address 1.2.0.2 255.255.255.252
[RouterB-Tunnel0] source loopback0
[RouterB-Tunnel0] destination 1.1.1.1
[RouterB-Tunnel0] quit
```
配置到 Router A 的环回口的静态路由，下一跳指向外网，并设置主备链路。
```
[RouterB] ip route-static 1.1.1.1 255.255.255.255 1.10.0.4
[RouterB] ip route-static 1.1.1.1 255.255.255.255 1.11.0.4 preference 100
```
配置到 Router A 内网的静态路由，下一跳为对端 GRE 隧道接口地址。
```
[RouterB] ip route-static 192.168.1.0 255.255.255.0 1.2.0.1
```
配置 ACL，定义由 192.168.2.0/24 到 192.168.1.0/24 的数据流。
```
[RouterB] acl number 3000
[RouterB-acl-adv-3000] rule 0 permit ip source 192.168.2.0 0.0.0.255 destination
 192.168.1.0 0.0.0.255
[RouterB-acl-adv-3000] quit
```
配置 IKE 对等体。
```
[RouterB] ike peer peer
[RouterB-ike-peer-peer] pre-shared-key 123
[RouterB-ike-peer-peer] remote-address 1.2.0.1
[RouterB-ike-peer-peer] quit
```
采用安全提议的缺省配置。
```
[RouterB] ipsec proposal def
[RouterB-ipsec-transform-set-def] esp authentication-algorithm md5
[RouterB-ipsec-transform-set-def] quit
```
配置 IPsec 安全策略 policy，其协商方式为 isakmp。
```
[RouterB] ipsec policy policy 1 isakmp
[RouterB-ipsec-policy-isakmp-policy-1] security acl 3000
[RouterB-ipsec-policy-isakmp-policy-1] ike-peer peer
[RouterB-ipsec-policy-isakmp-policy-1] proposal def
[RouterB-ipsec-policy-isakmp-policy-1] quit
```
在 GRE 隧道接口上应用安全策略。
```
[RouterB] interface tunnel 0
[RouterB-Tunnel0] ipsec policy policy
[RouterB-Tunnel0] quit
```

3.6 验证配置

完成以上配置后，GRE 隧道即可建立起来，且 IPsec 策略直接下发到 GRE 隧道，即使物理口 Down 掉，也不会影响内网之间的通信，这里以 Router A 为例进行验证。

在主备链路都完好的情况下，将以主链路进行通信。

```
<RouterA> display ip routing-table
Routing Tables: Public
         Destinations : 17       Routes : 17

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

1.1.1.1/32          Direct 0    0            127.0.0.1       InLoop0
1.2.0.0/30          Direct 0    0            1.2.0.1         Tun0
1.2.0.1/32          Direct 0    0            127.0.0.1       InLoop0
1.10.0.0/24         Direct 0    0            1.10.0.1        Eth0/0.10
1.10.0.1/32         Direct 0    0            127.0.0.1       InLoop0
1.11.0.0/24         Direct 0    0            1.11.0.1        Eth0/0.11
1.11.0.1/32         Direct 0    0            127.0.0.1       InLoop0
2.2.2.2/32          Static 60   0            1.10.0.2        Eth0/0.10
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
192.168.1.0/24      Direct 0    0            192.168.1.1     Vlan1
192.168.1.1/32      Direct 0    0            127.0.0.1       InLoop0
192.168.2.0/24      Static 60   0            1.2.0.2         Tun0
```

可以通过如下显示信息看到，内网主机间实现互通。

```
<RouterA> ping -a 192.168.1.1 192.168.2.1
  PING 192.168.2.1: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 192.168.2.1: bytes=56 Sequence=1 ttl=255 time=4 ms
    Reply from 192.168.2.1: bytes=56 Sequence=2 ttl=255 time=3 ms
    Reply from 192.168.2.1: bytes=56 Sequence=3 ttl=255 time=3 ms
    Reply from 192.168.2.1: bytes=56 Sequence=4 ttl=255 time=3 ms

  --- 192.168.2.1 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
round-trip min/avg/max = 3/3/4 ms
```

可以通过如下显示信息看到，GRE 隧道建立成功并有内网数据通过。

```
<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 1.2.0.1/30 Primary
Encapsulation is TUNNEL, service-loopback-group ID not set.
Tunnel source 1.1.1.1 (LoopBack0), destination 2.2.2.2
```

```
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:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    8 packets input,  1116 bytes
    0 input error
    18 packets output,  2204 bytes
    0 output error
```

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
  ----------------------------------------------------------------
     3             1.2.0.2                 RD|ST       1       IPSEC
     4             1.2.0.2                 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。

```
<RouterA> display ipsec sa
==============================
Interface: Tunnel0
    path MTU: 1476
==============================

  ----------------------------
  IPsec policy name: "policy"
  sequence number: 1
  acl version: ACL4
  mode: isakmp
  ----------------------------
    PFS: N, DH group: none
    tunnel:
        local  address: 1.2.0.1
        remote address: 1.2.0.2
    flow:
        sour addr: 192.168.1.0/255.255.255.0  port: 0  protocol: IP
        dest addr: 192.168.2.0/255.255.255.0  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 0x7FE5F3C0(2145776576)
```

```
    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): 1843199/3444
    anti-replay detection: Enabled
      anti-replay window size(counter based): 32
    udp encapsulation used for nat traversal: N

  [outbound ESP SAs]
    spi: 0x919FD949(2443172169)
    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): 1843199/3444
    anti-replay detection: Enabled
      anti-replay window size(counter based): 32
    udp encapsulation used for nat traversal: N
```

当主链路 Down 掉时，内网通信就会走备份链路。

```
<RouterA> display ip routing-table
Routing Tables: Public
         Destinations : 15       Routes : 15

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

1.1.1.1/32          Direct 0    0            127.0.0.1       InLoop0
1.2.0.0/30          Direct 0    0            1.2.0.1         Tun0
1.2.0.1/32          Direct 0    0            127.0.0.1       InLoop0
1.11.0.0/24         Direct 0    0            1.11.0.1        Eth0/0.11
1.11.0.1/32         Direct 0    0            127.0.0.1       InLoop0
2.2.2.2/32          Static 100  0            1.11.0.3        Eth0/0.11
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
192.168.1.0/24      Direct 0    0            192.168.1.1     Vlan1
192.168.1.1/32      Direct 0    0            127.0.0.1       InLoop0
192.168.2.0/24      Static 60   0            1.2.0.2         Tun0
```

但 GRE 隧道和 IPsec 并不受影响，内网之间仍然可以正常通信。显示同之前主链路完好情况，此不赘述。

3.7 配置文件

- Router A：

```
acl number 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
#
ike peer peer
 pre-shared-key cipher $c$3$dYGGPyImm2L0tVTrLDeYD4gN+1Q9AQ==
```

```
 remote-address 1.2.0.2
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy policy 1 isakmp
 security acl 3000
 ike-peer peer
 transform-set def
#
interface Ethernet0/0.10
 vlan-type dot1q vid 10
 ip address 1.10.0.1 255.255.255.0
#
interface Ethernet0/0.11
 vlan-type dot1q vid 11
 ip address 1.11.0.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface1
 ip address 192.168.1.1 255.255.255.0
#
interface Tunnel0
 ip address 1.2.0.1 255.255.255.252
 source LoopBack0
 destination 2.2.2.2
 ipsec policy policy
#
 ip route-static 2.2.2.2 255.255.255.255 1.10.0.2
 ip route-static 2.2.2.2 255.255.255.255 1.11.0.2 preference 100
 ip route-static 192.168.2.0 255.255.255.0 1.2.0.2
#
```

- Router B：

```
acl number 3000
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ike peer peer
 pre-shared-key cipher $c$3$XFqUNS4m0WNQNtbqFBucxhxZ5y/1xw==
 remote-address 1.2.0.1
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
```

```
#
ipsec policy policy 1 isakmp
 security acl 3000
 ike-peer peer
 transform-set def
#
interface Ethernet0/0.20
 vlan-type dot1q vid 20
 ip address 1.10.0.3 255.255.255.0
#
interface Ethernet0/0.21
 vlan-type dot1q vid 21
 ip address 1.11.0.3 255.255.255.0
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface1
 ip address 192.168.2.1 255.255.255.0
#
interface Tunnel0
 ip address 1.2.0.2 255.255.255.252
 source LoopBack0
 destination 1.1.1.1
 ipsec policy policy
#
 ip route-static 1.1.1.1 255.255.255.255 1.10.0.4
 ip route-static 1.1.1.1 255.255.255.255 1.11.0.4 preference 100
 ip route-static 192.168.1.0 255.255.255.0 1.2.0.1
#
```

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