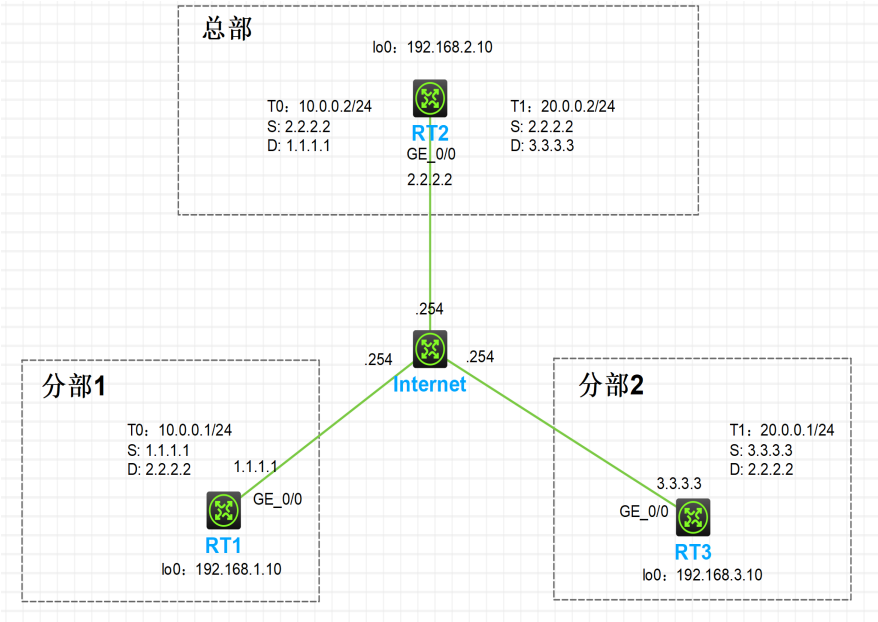
HCL模拟MSR V7平台路由器GRE over IPSec VPN多分支互通

IPSec VPN GRE VPN zhiliao_mg5WkO 2024-08-22 发表

组网及说明

1.组网拓扑



2.需求描述：

实现两个分部内网终端能够通过GRE over IPSec VPN隧道访问到总部，也能通过总部实现两个分部的内网终端互通。

分部与总部终端用loopback接口替代，ip地址固定。

3.配置思路：

配置各个端口ip地址与静态路由，配置GRE隧道与IPSec VPN相关命令实现流量的GRE封装，并通过IPSec隧道进行保护传输至目的地。

配置步骤

1.RT1

1.1ACL列表：

```
Advanced IPv4 ACL 3001, 2 rules,
ACL's step is 5
 rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255
 rule 1 permit ip source 1.1.1.0 0.0.0.255 destination 3.3.3.0 0.0.0.255

Advanced IPv4 ACL 3002, 3 rules,
ACL's step is 5
 rule 0 deny ip source 1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255
 rule 1 deny ip source 1.1.1.0 0.0.0.255 destination 3.3.3.0 0.0.0.255

 rule 2 permit ip
```

1.2 关键配置：

```
#
interface Tunnel0 mode gre
 ip address 10.0.0.1 255.255.255.0
 source 1.1.1.1
 destination 2.2.2.2
#
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy RT1 1 isakmp
 transform-set 1
 security acl 3001
```

```
 remote-address 2.2.2.2
 ike-profile RT1
#
ike profile RT1
 keychain RT1
 local-identity address 1.1.1.1
 match remote identity address 2.2.2.2 255.255.255.0
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain RT1
 pre-shared-key address 2.2.2.2 255.255.255.0 key cipher $c$3$SyBhccDEm/kTkb3J7k6o2PZq10DE
ypOVEg==
#
interface LoopBack0
 ip address 192.168.1.10 255.255.255.0
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 1.1.1.1 255.255.255.0
 nat outbound 3002
 ipsec apply policy RT1
#
 ip route-static 0.0.0.0 0 1.1.1.254
 ip route-static 192.168.2.0 24 Tunnel0
 ip route-static 192.168.3.0 24 Tunnel0
```

2.RT2

2.1ACL列表

```
Advanced IPv4 ACL 3001, 2 rules,
ACL's step is 5
 rule 0 permit ip source 2.2.2.0 0.0.0.255 destination 1.1.1.0 0.0.0.255
 rule 1 permit ip source 3.3.3.0 0.0.0.255 destination 1.1.1.0 0.0.0.255

Advanced IPv4 ACL 3002, 2 rules,
ACL's step is 5
 rule 0 permit ip source 2.2.2.0 0.0.0.255 destination 3.3.3.0 0.0.0.255
 rule 1 permit ip source 1.1.1.0 0.0.0.255 destination 3.3.3.0 0.0.0.255

Advanced IPv4 ACL 3003, 5 rules,
ACL's step is 5
 rule 0 deny ip source 2.2.2.0 0.0.0.255 destination 1.1.1.0 0.0.0.255
 rule 1 deny ip source 2.2.2.0 0.0.0.255 destination 3.3.3.0 0.0.0.255
 rule 2 deny ip source 1.1.1.0 0.0.0.255 destination 3.3.3.0 0.0.0.255
 rule 5 deny ip source 3.3.3.0 0.0.0.255 destination 1.1.1.0 0.0.0.255
 rule 6 permit ip
```

2.2关键配置：

```
#
interface Tunnel0 mode gre
 ip address 10.0.0.2 255.255.255.0
 source 2.2.2.2
 destination 1.1.1.1
#
interface Tunnel1 mode gre
 ip address 20.0.0.2 255.255.255.0
 source 2.2.2.2
 destination 3.3.3.3
#
ipsec transform-set 1
```

```
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy RT2 1 isakmp
 transform-set 1
 security acl 3001
 remote-address 1.1.1.1
 ike-profile RT2-RT1
#
ipsec policy RT2 2 isakmp
 transform-set 1
 security acl 3002
 remote-address 3.3.3.3
 ike-profile RT2-RT3
#
ike profile RT2-RT1
 keychain RT2-RT1
 local-identity address 2.2.2.2
 match remote identity address 1.1.1.1 255.255.255.0
 proposal 1
#
ike profile RT2-RT3
 keychain RT2-RT3
 local-identity address 2.2.2.2
 match remote identity address 3.3.3.3 255.255.255.0
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain RT2-RT1
 pre-shared-key address 1.1.1.1 255.255.255.0 key cipher $c$3$w74T8OIbosspb4Evy/1aSu3S+fb5S
UJjeA==
#
ike keychain RT2-RT3
 pre-shared-key address 3.3.3.3 255.255.255.0 key cipher $c$3$YDfVYtM49YVzXjOKCn8NQFd8yN/
D+Xpq2zzLZw==
#
interface LoopBack0
 ip address 192.168.2.10 255.255.255.0
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 2.2.2.2 255.255.255.0
 nat outbound 3003
 ipsec apply policy RT2
#
 ip route-static 0.0.0.0 0 2.2.2.254
 ip route-static 192.168.1.0 24 Tunnel0
 ip route-static 192.168.3.0 24 Tunnel1
```

3.RT3

3.1ACL列表：

```
Advanced IPv4 ACL 3001, 2 rules,
ACL's step is 5
 rule 0 permit ip source 3.3.3.0 0.0.0.255 destination 2.2.2.0 0.0.0.255
 rule 1 permit ip source 3.3.3.0 0.0.0.255 destination 1.1.1.0 0.0.0.255

Advanced IPv4 ACL 3002, 3 rules,
ACL's step is 5
 rule 0 deny ip source 3.3.3.0 0.0.0.255 destination 2.2.2.0 0.0.0.255
```

```
 rule 1 deny ip source 3.3.3.0 0.0.0.255 destination 1.1.1.0 0.0.0.255
 rule 2 permit ip
```

3.2关键配置：

```
#
interface Tunnel1 mode gre
 ip address 20.0.0.1 255.255.255.0
 source 3.3.3.3
 destination 2.2.2.2
#
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy RT3 1 isakmp
 transform-set 1
 security acl 3001
 remote-address 2.2.2.2
 ike-profile RT3
#
ike profile RT3
 keychain RT3
 local-identity address 3.3.3.3
 match remote identity address 2.2.2.2 255.255.255.0
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain RT3
 pre-shared-key address 2.2.2.2 255.255.255.0 key cipher $c$3$Fx1hsMm+uamipkMpvCFJr6wGrLO
RTkkBbgESOQ==
#
interface LoopBack0
 ip address 192.168.3.10 255.255.255.0
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 3.3.3.3 255.255.255.0
 nat outbound 3002
 ipsec apply policy RT3
#
 ip route-static 0.0.0.0 0 3.3.3.254
 ip route-static 192.168.1.0 24 Tunnel1
 ip route-static 192.168.2.0 24 Tunnel1
```

4.Internet

4.1关键配置：

```
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 1.1.1.254 255.255.255.0
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 3.3.3.254 255.255.255.0
#
interface GigabitEthernet0/2
 port link-mode route
 combo enable copper
```

```
 ip address 2.2.2.254 255.255.255.0
#
 ip route-static 192.168.1.0 24 1.1.1.1
 ip route-static 192.168.2.0 24 2.2.2.2
 ip route-static 192.168.3.0 24 3.3.3.3
```

5.测试

RT1内网终端（分部1）ping通RT2内网终端（总部）

```
<RT1>ping -a 192.168.1.10 192.168.2.10
Ping 192.168.2.10 (192.168.2.10) from 192.168.1.10: 56 data bytes, press CTRL+C to break
56 bytes from 192.168.2.10: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 192.168.2.10: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 192.168.2.10: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 192.168.2.10: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 192.168.2.10: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 192.168.2.10 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
<RT1>%Aug 22 12:47:08:590 2024 RT1 PING/6/PING_STATISTICS: Ping statistics for 192.168.2.10: 5 packe
t(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/std-dev = 1.000/1.2
00/2.000/0.400 ms.
```

RT1内网终端（分部1）ping通RT3内网终端（分部2）

```
<RT1>ping -a 192.168.1.10 192.168.3.10
Ping 192.168.3.10 (192.168.3.10) from 192.168.1.10: 56 data bytes, press CTRL+C to break
56 bytes from 192.168.3.10: icmp_seq=0 ttl=254 time=3.000 ms
56 bytes from 192.168.3.10: icmp_seq=1 ttl=254 time=3.000 ms
56 bytes from 192.168.3.10: icmp_seq=2 ttl=254 time=2.000 ms
56 bytes from 192.168.3.10: icmp_seq=3 ttl=254 time=2.000 ms
56 bytes from 192.168.3.10: icmp_seq=4 ttl=254 time=3.000 ms

--- Ping statistics for 192.168.3.10 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.000/2.600/3.000/0.490 ms
<RT1>%Aug 22 12:47:15:671 2024 RT1 PING/6/PING_STATISTICS: Ping statistics for 192.168.3.10: 5 packe
t(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/std-dev = 2.000/2.6
00/3.000/0.490 ms.
```

RT2总部查看ike sa与ipsec sa相关信息：

```
 <RT2>dis ike sa
   Connection-ID   Local            Remote           Flag      DOI
--------------------------------------------------------------------------------
   1               2.2.2.2          1.1.1.1          RD        IPsec
   2               2.2.2.2          3.3.3.3          RD        IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY

<RT2>dis ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------


  -----------------------------
  IPsec policy: RT2-RT1
  Sequence number: 1
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Transmitting entity: Responder
    Path MTU: 1444
    Tunnel:
        local  address: 2.2.2.2
        remote address: 1.1.1.1
    Flow:
```

```
    sour addr: 2.2.2.0/255.255.255.0  port: 0  protocol: ip
    dest addr: 1.1.1.0/255.255.255.0  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 3085965188 (0xb7f01784)
    Connection ID: 4294967296
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843197/3577
    Max received sequence-number: 19
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

  [Outbound ESP SAs]
    SPI: 3622549341 (0xd7ebb75d)
    Connection ID: 4294967297
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843198/3577
    Max sent sequence-number: 18
    UDP encapsulation used for NAT traversal: N
    Status: Active

------------------------------
IPsec policy: RT2-RT1
Sequence number: 2
Mode: ISAKMP
------------------------------
  Tunnel id: 1
  Encapsulation mode: tunnel
  Perfect Forward Secrecy:
  Inside VPN:
  Extended Sequence Numbers enable: N
  Traffic Flow Confidentiality enable: N
  Transmitting entity: Initiator
  Path MTU: 1444
  Tunnel:
      local  address: 2.2.2.2
      remote address: 3.3.3.3
  Flow:
      sour addr: 2.2.2.0/255.255.255.0  port: 0  protocol: ip
      dest addr: 3.3.3.0/255.255.255.0  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 1899742260 (0x713bc434)
    Connection ID: 4294967298
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3587
    Max received sequence-number: 9
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

  [Outbound ESP SAs]
    SPI: 62185102 (0x03b4de8e)
    Connection ID: 4294967299
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3587
    Max sent sequence-number: 9
```

UDP encapsulation used for NAT traversal: N
Status: Active

配置关键点

1.如果之前已经在外网口配置了 nat outbound，需要先undo掉
2.隧道两端注意加密算法和认证算法的统一
3.注意创建相关正确的ACL，把IPSec感兴趣流从NAT转换的数据deny掉，防止IPSec数据流被NAT优先转换
4.ipsec policy RT2中创建序列号为1和2分别用于目的为分部1和分部2的策略