IPsec Over MPLS典型配置

马文斌 2017-08-21 发表

一、 组网需求：

某客户组网如下图所示，客户两个局点之间是MPLS网络，客户希望在CE之间再增加一层IPsec隧道保护内部流量。

二、 组网图：

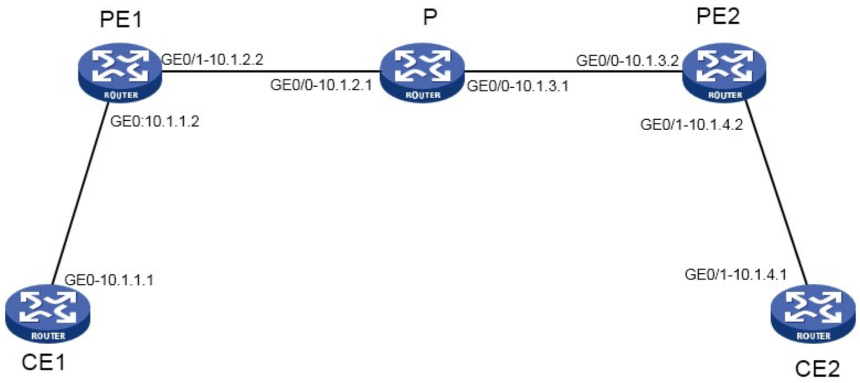

图1

如图，PE1—PE2之间跑MPLS网络，客户还希望在CE1和CE2之间跑IPsec隧道加密报文

三、配置步骤：

首先在各个路由器接口正确的配置IP，并且配置路由协议，使得各个网段可以互达。

PE1、P、PE2的Loopback接口分别为1.1.1.1、2.2.2.2、3.3.3.3

然后在PE1、P、PE2之间开启ospf和MPLS功能：

【PE1】

```
#
ip vpn-instance 1  //配置VPN信息
 route-distinguisher 1:1  //RD为1:1
 vpn-target 1:1 import-extcommunity  //RT也是1:1
 vpn-target 1:1 export-extcommunity
#
ospf 1  //配置ospf发布公网路由
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
#
 mpls lsr-id 1.1.1.1  //配置mpls lsr-id
#
mpls ldp  //全局开启mpls ldp
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip binding vpn-instance 1  //连接CE的接口绑定VPN 1
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 10.1.2.2 255.255.255.0
 ospf network-type p2p
 mpls enable  //连接P设备接口启用mpls和mpls ldp
 mpls ldp enable
#
bgp 100  //配置bgp
 peer 3.3.3.3 as-number 100
 peer 3.3.3.3 connect-interface LoopBack0
 #
 address-family vpnv4
  peer 3.3.3.3 enable
 #
 ip vpn-instance 1
  #
  address-family ipv4 unicast
   import-route direct  //引入直连
#
【P】
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 10.1.3.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
 mpls lsr-id 2.2.2.2
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 10.1.2.1 255.255.255.0
 ospf network-type p2p
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 10.1.3.1 255.255.255.0
 ospf network-type p2p
 mpls enable
 mpls ldp enable
#
【PE2】
#
ip vpn-instance 1
 route-distinguisher 1:1
 vpn-target 1:1 import-extcommunity
 vpn-target 1:1 export-extcommunity
#
ospf 1
 area 0.0.0.0
  network 10.1.3.0 0.0.0.255
  network 3.3.3.3 0.0.0.0
#
 mpls lsr-id 3.3.3.3
#
mpls ldp
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 10.1.3.2 255.255.255.0
 ospf network-type p2p
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip binding vpn-instance 1
 ip address 10.1.4.2 255.255.255.0
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack0
 #
 address-family vpnv4
  peer 1.1.1.1 enable
 #
 ip vpn-instance 1
  #
  address-family ipv4 unicast
   import-route direct
#
```

【CE1】

```
#
acl advanced 3000
 rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.4.0 0.0.0.255
#
ipsec transform-set 1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm md5
#
ike profile 1
 keychain 1
 match remote identity address 10.1.4.1 255.255.255.255
#
ike keychain 1
 pre-shared-key address 10.1.4.1 255.255.255.255 key cipher $c$3$i9oITggPMsgflovTP3MRJUch3P
ZkFkIH/w==
#
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3000
 remote-address 10.1.4.1
 ike-profile 1
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 10.1.1.1 255.255.255.0
 ipsec apply policy 1
#
ip route-static 0.0.0.0 0 10.1.1.2
#
```

【CE2】

```
#
acl advanced 3000
 rule 0 permit ip source 10.1.4.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec transform-set 1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm md5
#
ike profile 1
```

```
 keychain 1
 match remote identity address 10.1.1.1 255.255.255.255
#
ike keychain 1
 pre-shared-key address 10.1.1.1 255.255.255.255 key cipher $c$3$AhfWOkT8fhAylzfJxgUpdw9/yoc
dIXINZw==
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3000
 remote-address 10.1.1.1
 ike-profile 1
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 10.1.4.1 255.255.255.0
 ipsec apply policy 1
#
 ip route-static 0.0.0.0 0 10.1.4.2
#
```

【在PE1上查看BGP邻居信息】

```
<PE1>display bgp peer vpnv4

 BGP local router ID: 1.1.1.1
 Local AS number: 100
 Total number of peers: 1                Peers in established state: 1

  * - Dynamically created peer
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  3.3.3.3                100       52       50    0       1 00:39:50 Established
```

【在PE1上查看vpnv4路由信息】

```
[PE1]display bgp routing-table vpnv4

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PEs: 1

 Route distinguisher: 1:1(1)
 Total number of routes: 3

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >  10.1.1.0/24        10.1.1.2        0                     32768   ?
* >  10.1.1.2/32        127.0.0.1       0                     32768   ?
* >i 10.1.4.0/24        3.3.3.3         0          100        0       ?   //学到了对端PE2的私网路由
```

【CE1上ping CE2触发IPsec建立】

```
[CE1]ping -a 10.1.1.1 10.1.4.1
Ping 10.1.4.1 (10.1.4.1) from 10.1.1.1: 56 data bytes, press CTRL_C to break
Request time out  //丢一个包，说明IPsec建立
56 bytes from 10.1.4.1: icmp_seq=1 ttl=255 time=3.000 ms
56 bytes from 10.1.4.1: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 10.1.4.1: icmp_seq=3 ttl=255 time=3.000 ms
56 bytes from 10.1.4.1: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for 10.1.4.1 ---
5 packet(s) transmitted, 4 packet(s) received, 20.0% packet loss
round-trip min/avg/max/std-dev = 2.000/2.500/3.000/0.500 ms
```

【查看ike sa和IPsec sa】

```
[CE1]dis ike sa
    Connection-ID   Remote              Flag        DOI
------------------------------------------------------------------
7              10.1.4.1             RD          IPsec

[CE1]dis ipsec sa
-----------------------------
  IPsec policy: 1
  Sequence number: 1
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 1
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1444
    Tunnel:
        local  address: 10.1.1.1
        remote address: 10.1.4.1
    Flow:
        sour addr: 10.1.1.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 10.1.4.0/255.255.255.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 851573583 (0x32c1fb4f)
      Connection ID: 4294967298
      Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3536
      Max received sequence-number: 4
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 402872853 (0x18035a15)
      Connection ID: 4294967299
      Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3536
      Max sent sequence-number: 4
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

四、 配置关键点:

由于IPsec是在CE之间建立，所以中间MPLS网络可以不予考虑，只要CE1和CE2的路由可达即可建立IPsec隧道