分支数据通过ipsec加密，但是之间不建立ispec邻居

IPSec VPN　樊凡　2019-10-30 发表

问题描述

分支数据通过ipsec加密，但是之间不建立ispec邻居

解决方法

```
 R1--LO:111.111.111.111
          1.1.1.2  |
                   |
          1.1.1.1  |
                  SW
        2.2.2.1  /   \3.3.3.1
               /     \
        2.2.2.2/       \3.3.3.2
             R2        R3---L0:33.33.33.33
             |
            LO:222.222.222.222
```

R2和R3分别和总部R1建立ipsec隧道，但是R2和R3之间不建立ipsec邻居关系，但是R2和R3之间的流量要通过ipsec加密。

R1配置:

```
acl number 3000
 rule 0 permit ip source 111.111.111.111 0 destination 222.222.222.222 0
 rule 5 permit ip source 33.33.33.33 0 destination 222.222.222.222 0
acl number 3001
 rule 0 permit ip source 222.222.222.222 0 destination 33.33.33.33 0
 rule 5 permit ip source 111.111.111.111 0 destination 33.33.33.33 0
#
ike peer r1
#
ike peer r2
 pre-shared-key simple h3c
 remote-address 2.2.2.2
#
ike peer r3
 pre-shared-key simple h3c
 remote-address 3.3.3.2
#
ipsec proposal 1
#
ipsec proposal 2
#
ipsec policy h3c 1 isakmp
 security acl 3000
 ike-peer r2
 proposal 1
#
ipsec policy h3c 2 isakmp
 security acl 3001
 ike-peer r3
 proposal 2

interface LoopBack0
 ip address 111.111.111.111 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 1.1.1.2 255.255.255.0
 ipsec policy h3c

ip route-static 0.0.0.0 0.0.0.0 1.1.1.1 preference 80
```

```
<r1>dis ike sa
  total phase-1 SAs:  2
  connection-id  peer           flag       phase   doi
 -----------------------------------------------------------------
    31           2.2.2.2        RD          2     IPSEC
    30           3.3.3.2        RD          2     IPSEC
    29           3.3.3.2        RD          2     IPSEC
    28           3.3.3.2        RD          1     IPSEC
    22           2.2.2.2        RD          1     IPSEC
    32           2.2.2.2        RD          2     IPSEC

<r1>dis ipsec sa brief
 total phase-2 SAs: 8
Src Address     Dst Address     SPI         Protocol  Algorithm
-----------------------------------------------------------------
1.1.1.2         2.2.2.2         4259480772 ESP       E:DES
                                           A:HMAC-MD5-96
2.2.2.2         1.1.1.2         1242179900 ESP       E:DES
                                           A:HMAC-MD5-96
1.1.1.2         2.2.2.2         371154342  ESP       E:DES
                                           A:HMAC-MD5-96
1.1.1.2         3.3.3.2         3660672503 ESP       E:DES
                                           A:HMAC-MD5-96
2.2.2.2         1.1.1.2         2724522547 ESP       E:DES
                                           A:HMAC-MD5-96
1.1.1.2         3.3.3.2         2344403602 ESP       E:DES
                                           A:HMAC-MD5-96
3.3.3.2         1.1.1.2         1250871088 ESP       E:DES
                                           A:HMAC-MD5-96
3.3.3.2         1.1.1.2         911910764  ESP       E:DES
                                           A:HMAC-MD5-96
```

R2配置：

```
acl number 3000
 rule 0 permit ip source 222.222.222.222 0 destination 111.111.111.111 0
 rule 5 permit ip source 222.222.222.222 0 destination 33.33.33.33 0

ike peer r1
 pre-shared-key simple h3c
 remote-address 1.1.1.2
#
ipsec proposal 1
#
ipsec policy h3c 1 isakmp
 security acl 3000
 ike-peer r1
 proposal 1
interface LoopBack0
 ip address 222.222.222.222 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 2.2.2.2 255.255.255.0
 ipsec policy h3c
#
 ip route-static 0.0.0.0 0.0.0.0 2.2.2.1 preference 80

<r2>dis ike sa
  total phase-1 SAs:  1
  connection-id  peer           flag       phase   doi
```

```
  ------------------------------------------------------------------
    13          1.1.1.2         RD|ST        2     IPSEC
    11          1.1.1.2         RD|ST        1     IPSEC
    14          1.1.1.2         RD|ST        2     IPSEC

<r2>dis ipsec sa brief
 total phase-2 SAs: 4
Src Address     Dst Address     SPI         Protocol  Algorithm
-----------------------------------------------------------------------
1.1.1.2         2.2.2.2         4259480772 ESP       E:DES
                                           A:HMAC-MD5-96
2.2.2.2         1.1.1.2         1242179900 ESP       E:DES
                                           A:HMAC-MD5-96
1.1.1.2         2.2.2.2         371154342  ESP       E:DES
                                           A:HMAC-MD5-96
2.2.2.2         1.1.1.2         2724522547 ESP       E:DES
                                           A:HMAC-MD5-96

<r2>ping -a 222.222.222.222 33.33.33.33
  PING 33.33.33.33: 56  data bytes, press CTRL_C to break
    Reply from 33.33.33.33: bytes=56 Sequence=1 ttl=254 time=3 ms
    Reply from 33.33.33.33: bytes=56 Sequence=2 ttl=254 time=3 ms
    Reply from 33.33.33.33: bytes=56 Sequence=3 ttl=254 time=3 ms
    Reply from 33.33.33.33: bytes=56 Sequence=4 ttl=254 time=2 ms
    Reply from 33.33.33.33: bytes=56 Sequence=5 ttl=254 time=3 ms

  --- 33.33.33.33 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/3 ms

R3配置:
acl number 3000
 rule 0 permit ip source 33.33.33.33 0 destination 111.111.111.111 0
 rule 5 permit ip source 33.33.33.33 0 destination 222.222.222.222 0

ike peer r1
 pre-shared-key simple h3c
 remote-address 1.1.1.2
#
ipsec proposal 1
#
ipsec policy h3c 1 isakmp
 security acl 3000
 ike-peer r1
 proposal 1

interface LoopBack0
 ip address 33.33.33.33 255.255.255.255

interface GigabitEthernet0/1
 port link-mode route
 ip address 3.3.3.2 255.255.255.0
 ipsec policy h3c

 ip route-static 0.0.0.0 0.0.0.0 3.3.3.1

<r3>
<r3>dis ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  ------------------------------------------------------------------
    18          1.1.1.2         RD|ST        1     IPSEC
```

```
    20          1.1.1.2         RD|ST       2     IPSEC
    21          1.1.1.2         RD|ST       2     IPSEC

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

<r3>dis ipsec sa brief
 total phase-2 SAs: 4
Src Address     Dst Address     SPI         Protocol  Algorithm
------------------------------------------------------------------------------
3.3.3.2         1.1.1.2         4160065659 ESP       E:DES
                                           A:HMAC-MD5-96
1.1.1.2         3.3.3.2         3344377081 ESP       E:DES
                                           A:HMAC-MD5-96
1.1.1.2         3.3.3.2         2344403602 ESP       E:DES
                                           A:HMAC-MD5-96
3.3.3.2         1.1.1.2         911910764  ESP       E:DES
                                           A:HMAC-MD5-96
<r3>ping -a 33.33.33.33 222.222.222.222
  PING 222.222.222.222: 56  data bytes, press CTRL_C to break
    Reply from 222.222.222.222: bytes=56 Sequence=1 ttl=254 time=3 ms
    Reply from 222.222.222.222: bytes=56 Sequence=2 ttl=254 time=2 ms
    Reply from 222.222.222.222: bytes=56 Sequence=3 ttl=254 time=3 ms
    Reply from 222.222.222.222: bytes=56 Sequence=4 ttl=254 time=2 ms
    Reply from 222.222.222.222: bytes=56 Sequence=5 ttl=254 time=2 ms

  --- 222.222.222.222 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/3 ms
```