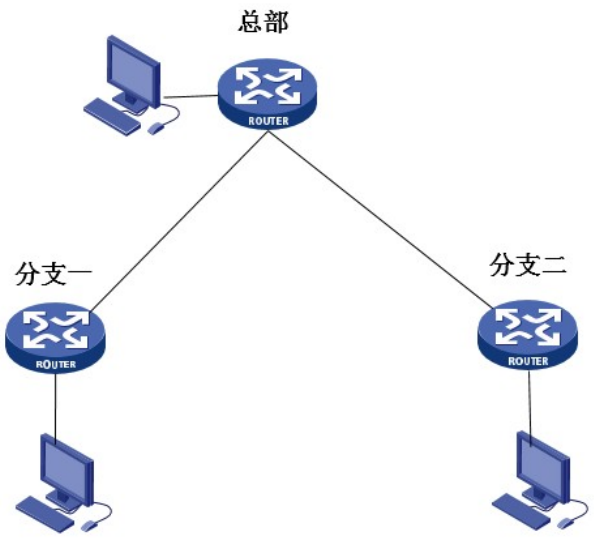
IPsec多分支经由总部互通

IPsec　朱玉广　2015-11-05 发表

1、总部采用MSR56设备，分支采用MSR36和MSR30
2、分支和总部之间起IPsec；
3、分支之间不直接建立IPsec，经由总部IPsec VPN实现分支互通。



总部PC地址为：3.3.3.3
分支一PC地址为：2.2.2.2
分支二PC地址为：4.4.4.4

首先配置总部设备：
#这里在总部设备上起一个loopback接口，来模仿PC。
[H3C]interface LoopBack0
[H3C-LoopBack0] ip address 3.3.3.3 255.255.255.255
#这里先配置IKE Keychain，配置与分支之间协商采用的预共享密钥，由于分支设备无公网IP，这里需要采用name的方式，这里配置分支一的name为123，分支的name为234，分支name需要与分支侧设置的一致。
[H3C]ike keychain 123
[H3C-ike-keychain-123] pre-shared-key hostname 123 key simple 123456
[H3C-ike-keychain-123] quit
[H3C]ike keychain 235
[H3C-ike-keychain-235] pre-shared-key hostname 234 key simple 123456

#配置两个分支对应的IKE Profile，调用配置的ike keychain，采用野蛮模式，并分别匹配对端配置的ike name。
[H3C]ike profile 123
[H3C-ike-profile-123] keychain 123
[H3C-ike-profile-123] exchange-mode aggressive
[H3C-ike-profile-123] local-identity fqdn center
[H3C-ike-profile-123] match remote identity fqdn 123
[H3C-ike-profile-123] quit
[H3C]ike profile 333
[H3C-ike-profile-333] keychain 235
[H3C-ike-profile-333] exchange-mode aggressive
[H3C-ike-profile-333] local-identity fqdn center
[H3C-ike-profile-333] match remote identity fqdn 234
[H3C-ike-profile-333]

#配置IPsec安全提议，这里加密方式采用des，验证方式采用md5
[H3C]ipsec transform-set 123
[H3C-ipsec-transform-set-123] esp encryption-algorithm des-cbc
[H3C-ipsec-transform-set-123] esp authentication-algorithm md5

#配置安全ACL，匹配感兴趣流，这里的配置非常重要，尽管分支一和分支二之间并不直接建立ipsec，然后还是需要在ACL中对分支一到分支二的内网流量进行匹配，这一点非常重要。
分支1：
acl number 3000
 rule 0 permit ip source 3.3.3.3 0 destination 2.2.2.2 0
 rule 5 permit ip source 4.4.4.4 0 destination 2.2.2.2 0
分支2：
acl number 3001
 rule 0 permit ip source 2.2.2.2 0 destination 4.4.4.4 0
 rule 5 permit ip source 3.3.3.3 0 destination 4.4.4.4 0

#配置IPsec策略，这里采用IPsec策略模板的方式，分别配置对应分支的IPsec安全提议和安全ACL。
分支1：
[H3C]ipsec policy-template 234 1
[H3C-ipsec-policy-template-234-1] transform-set 123
[H3C-ipsec-policy-template-234-1] security acl 3000
[H3C-ipsec-policy-template-234-1] ike-profile 123
分支2：
[H3C]ipsec policy-template 333 1
[H3C-ipsec-policy-template-333-1] transform-set 123
[H3C-ipsec-policy-template-333-1] security acl 3001
[H3C-ipsec-policy-template-333-1] ike-profile 333
[H3C-ipsec-policy-template-333-1]quit

#使用ipsec策略调用配置的IPsec策略模板：
[H3C]ipsec policy 456 1 isakmp template 234
[H3C]ipsec policy 456 2 isakmp template 333

#配置完成之后，将ipsec策略下发到接口上：
[H3C]interface GigabitEthernet0/0
[H3C-GigabitEthernet0/0] ip address 1.1.1.2 255.255.255.0
[H3C-GigabitEthernet0/0] ipsec apply policy 456

配置分支：
配置分支一
#在分支一上同样使用了一个loopback接口模仿PC 3.3.3.3：
[H3C]interface LoopBack0
[H3C-LoopBack0] ip address 2.2.2.2 255.255.255.255
#配置设备对应的共享密钥
[H3C]ike keychain 123
[H3C-ike-keychain-123] pre-shared-key address 1.1.1.2 255.255.255.255 simple 123456
#配置本设备的ike name标识为123
[H3C] ike identity fqdn 123
#配置ike profile，调用配置的ike keychain，并采用野蛮模式。
[H3C]ike profile 123
[H3C-ike-profile-123] keychain 123
[H3C-ike-profile-123] exchange-mode aggressive
[H3C-ike-profile-123] local-identity fqdn 123
[H3C-ike-profile-123] match remote identity fqdn center
#配置IPsec安全提议，设备加密类型为des，验证类型为md5，这里需要与总部的保持一致。
[H3C]ipsec transform-set 123
[H3C-ipsec-transform-set-123] esp encryption-algorithm des-cbc
[H3C-ipsec-transform-set-123] esp authentication-algorithm md5
#配置ACL，这里在匹配分支到总部的流量之外，还需要匹配下分支一到分支二的内网流量。
acl number 3000
 rule 0 permit ip source 2.2.2.2 0 destination 3.3.3.3 0
 rule 5 permit ip source 2.2.2.2 0 destination 4.4.4.4 0

#配置ipsec策略，调用设备配置的ACL感兴趣流
[H3C]ipsec policy 123 1 isakmp
[H3C-ipsec-policy-isakmp-123-1] transform-set 123
[H3C-ipsec-policy-isakmp-123-1] security acl 3000
[H3C-ipsec-policy-isakmp-123-1] remote-address 1.1.1.2

[H3C-ipsec-policy-isakmp-123-1] ike-profile 123
#在接口下发ipsec策略。
[H3C]interface GigabitEthernet0/0
[H3C-GigabitEthernet0/0] ip address 1.1.1.1 255.255.255.0
[H3C-GigabitEthernet0/0] ipsec apply policy 123

配置分支二：
#分支二采用了V5设备，首先配置ike peer，配置预共享密钥，并使用野蛮模式，本地ike name设置为234
[test]ike peer 123
[test-ike-peer-123] exchange-mode aggressive
[test-ike-peer-123] pre-shared-key simple 123456
[test-ike-peer-123] id-type name
[test-ike-peer-123] remote-name center
[test-ike-peer-123] remote-address 1.1.1.2
[test-ike-peer-123] local-name 234
#配置IPsec感兴趣流，这一点很重要，尤其注意红色标记部分：
acl number 3000
 rule 0 permit ip source 4.4.4.4 0 destination 2.2.2.2 0
 rule 5 permit ip source 4.4.4.4 0 destination 3.3.3.3 0

#配置IPsec安全提议，并配置与总部设备一致的加密和验证算法
[test]ipsec transform-set 123
[test-ipsec-transform-set-123] encapsulation-mode tunnel
[test-ipsec-transform-set-123] transform esp
[test-ipsec-transform-set-123] esp authentication-algorithm md5
[test-ipsec-transform-set-123] esp encryption-algorithm des

#配置IPsec策略，调用配置的ACL感兴趣流和IPsec安全提议以及ike peer
[test]ipsec policy 123 1 isakmp
[test-ipsec-policy-isakmp-123-1] security acl 3000
[test-ipsec-policy-isakmp-123-1] ike-peer 123
[test-ipsec-policy-isakmp-123-1] transform-set 123

#然后将ipsec策略下发到接口之上：
[test]interface Ethernet0/5
[test-Ethernet0/5] port link-mode route
[test-Ethernet0/5] ip address 1.1.1.4 255.255.255.0
[test-Ethernet0/5] ipsec policy 123

配置完成之后，
做如下两件事儿：
    1、从分支一分别带源ping总部的3.3.3.3和分支二的4.4.4.4地址
    2、从分支二分别带源ping总部的3.3.3.3和分支一的2.2.2.2地址
接着查看ike和ipsec sa信息：

分支一：
通过配置可以看到分支一和分支二已经经由总部建立起了IPsec。
[RT1]dis ike sa
   Connection-ID   Remote   Flag   DOI
----
   9   1.1.1.2   RD   IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
[RT1]dis ips
[RT1]dis ipsec sa

Interface: GigabitEthernet0/0

  IPsec policy: 123
  Sequence number: 1

```
Mode: isakmp
-----------------------------
  Tunnel id: 0
  Encapsulation mode: tunnel
  Perfect forward secrecy:
  Path MTU: 1443
  Tunnel:
      local  address: 1.1.1.1
      remote address: 1.1.1.2
  Flow:
  sour addr: 2.2.2.2/255.255.255.255  port: 0  protocol: ip
  dest addr: 4.4.4.4/255.255.255.255  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 3617694698 (0xd7a1a3ea)
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3474
    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: 943654329 (0x383f05b9)
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3474
    Max sent sequence-number: 4
    UDP encapsulation used for NAT traversal: N
    Status: active

------------------------------
IPsec policy: 123
Sequence number: 1
Mode: isakmp
-----------------------------
  Tunnel id: 1
  Encapsulation mode: tunnel
  Perfect forward secrecy:
  Path MTU: 1443
  Tunnel:
      local  address: 1.1.1.1
      remote address: 1.1.1.2
  Flow:
  sour addr: 2.2.2.2/255.255.255.255  port: 0  protocol: ip
  dest addr: 3.3.3.3/255.255.255.255  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 2875326976 (0xab620200)
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3591
    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: 3491179830 (0xd0172d36)
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
```

SA remaining duration (kilobytes/sec): 1843199/3591
Max sent sequence-number: 4
UDP encapsulation used for NAT traversal: N
Status: active

此时分支一带源ping分支二地址，可以看到：

[RT1]ping -a 2.2.2.2 4.4.4.4
Ping 4.4.4.4 (4.4.4.4) from 2.2.2.2: 56 data bytes, press CTRL_C to break
56 bytes from 4.4.4.4: icmp_seq=0 ttl=254 time=1.979 ms
56 bytes from 4.4.4.4: icmp_seq=1 ttl=254 time=1.665 ms
56 bytes from 4.4.4.4: icmp_seq=2 ttl=254 time=1.372 ms
56 bytes from 4.4.4.4: icmp_seq=3 ttl=254 time=1.367 ms
56 bytes from 4.4.4.4: icmp_seq=4 ttl=254 time=1.374 ms

--- Ping statistics for 4.4.4.4 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.367/1.551/1.979/0.242 ms

在分支二上做ping测试，可以看出，ipsec VPN已经完全建立起来。

ping -a 4.4.4.4 3.3.3.3
PING 3.3.3.3: 56 data bytes, press CTRL_C to break
Reply from 3.3.3.3: bytes=56 Sequence=0 ttl=255 time=3 ms
Reply from 3.3.3.3: bytes=56 Sequence=1 ttl=255 time=1 ms
Reply from 3.3.3.3: bytes=56 Sequence=2 ttl=255 time=2 ms
Reply from 3.3.3.3: bytes=56 Sequence=3 ttl=255 time=2 ms
Reply from 3.3.3.3: bytes=56 Sequence=4 ttl=255 time=2 ms

--- 3.3.3.3 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/2/3 ms

ping -a 4.4.4.4 2.2.2.2
PING 2.2.2.2: 56 data bytes, press CTRL_C to break
Reply from 2.2.2.2: bytes=56 Sequence=0 ttl=254 time=3 ms
Reply from 2.2.2.2: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=254 time=2 ms
Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=254 time=2 ms
Reply from 2.2.2.2: bytes=56 Sequence=4 ttl=254 time=2 ms

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

这时，可以查看下总部设备上的ike和ipsec sa信息，

dis ike sa
Connection-ID Remote Flag DOI
---
21 1.1.1.4 RD IPSEC
19 1.1.1.1 RD IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
dis ips
dis ipsec sa

Interface: GigabitEthernet0/0

IPsec policy: 456
Sequence number: 1

```
Mode: template
-----------------------------
  Tunnel id: 0
  Encapsulation mode: tunnel
  Perfect forward secrecy:
  Path MTU: 1443
  Tunnel:
      local  address: 1.1.1.2
      remote address: 1.1.1.1
  Flow:
  sour addr: 4.4.4.4/255.255.255.255  port: 0  protocol: ip
  dest addr: 2.2.2.2/255.255.255.255  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 943654329 (0x383f05b9)
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843198/3352
    Max received sequence-number: 14
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: active

  [Outbound ESP SAs]
    SPI: 3617694698 (0xd7a1a3ea)
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843198/3352
    Max sent sequence-number: 14
    UDP encapsulation used for NAT traversal: N
    Status: active

-----------------------------
IPsec policy: 456
Sequence number: 1
Mode: template
-----------------------------
  Tunnel id: 3
  Encapsulation mode: tunnel
  Perfect forward secrecy:
  Path MTU: 1443
  Tunnel:
      local  address: 1.1.1.2
      remote address: 1.1.1.1
  Flow:
  sour addr: 3.3.3.3/255.255.255.255  port: 0  protocol: ip
  dest addr: 2.2.2.2/255.255.255.255  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 3491179830 (0xd0172d36)
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3469
    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: 2875326976 (0xab620200)
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
```

```
    SA remaining duration (kilobytes/sec): 1843199/3469
    Max sent sequence-number: 4
    UDP encapsulation used for NAT traversal: N
    Status: active

------------------------------
IPsec policy: 456
Sequence number: 2
Mode: template
------------------------------
  Tunnel id: 1
  Encapsulation mode: tunnel
  Perfect forward secrecy:
  Path MTU: 1443
  Tunnel:
      local  address: 1.1.1.2
      remote address: 1.1.1.4
  Flow:
  sour addr: 3.3.3.3/255.255.255.255  port: 0  protocol: ip
  dest addr: 4.4.4.4/255.255.255.255  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 3819554622 (0xe3a9c73e)
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3229
    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: 593870233 (0x2365bd99)
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3229
    Max sent sequence-number: 9
    UDP encapsulation used for NAT traversal: N
    Status: active

------------------------------
IPsec policy: 456
Sequence number: 2
Mode: template
------------------------------
  Tunnel id: 2
  Encapsulation mode: tunnel
  Perfect forward secrecy:
  Path MTU: 1443
  Tunnel:
      local  address: 1.1.1.2
      remote address: 1.1.1.4
  Flow:
  sour addr: 2.2.2.2/255.255.255.255  port: 0  protocol: ip
  dest addr: 4.4.4.4/255.255.255.255  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 648605780 (0x26a8f054)
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843198/3258
    Max received sequence-number: 18
    Anti-replay check enable: Y
```

Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: active

[Outbound ESP SAs]
SPI: 4111189432 (0xf50bc5b8)
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843198/3258
Max sent sequence-number: 14
UDP encapsulation used for NAT traversal: N
Status: active

1、当分支之间无公网地址时，需要采用野蛮模式；
2、配置时，一定要配置分支到分支的感兴趣流；
3、Ping触发时，需要分支间双向进行ping触发，才能同时建立起ipsec vpn，并实现经由总部互通
。