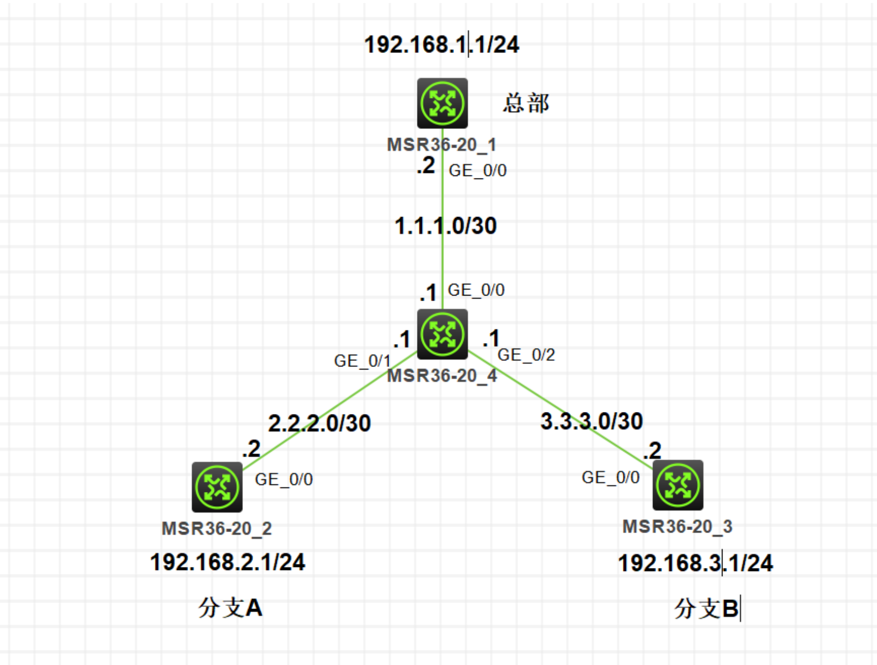
ipsec多分支互访+分支自动触发隧道建立

IPSec VPN NQA **胡琪** 2020-06-16 发表

组网及说明

1、组网



2、需求

建立ipsec vpn实现各分支和总部之间互通，并且各分支之间也能通过总部访问。总部是固定ip地址，分支IP地址不固定，并且分支A、B处无人值守且分支无主动自动访问总部的业务运行，所以为了防止分支设备断电重启后无法主动建立隧道，需要通过NQA来实现设备断电重启后自动触发隧道建立。

配置步骤

3、关键配置

总部：

```
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 1.1.1.2 255.255.255.252
 nat outbound 3002
 ipsec apply policy test
#
 ip route-static 0.0.0.0 0 1.1.1.1
#
acl advanced 3000
 description toBranchA
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
 rule 5 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
#
acl advanced 3001
 description toBranchB
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
 rule 5 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
#
acl advanced 3002
 description outboundNATDenyFlow
 rule 0 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
 rule 5 deny ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
 rule 10 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
 rule 15 deny ip source 192.168.2.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
 rule 100 permit ip
#
```

```
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy-template branchA 1
 transform-set 1
 security acl 3000
 ike-profile branchA
#
ipsec policy-template branchB 1
 transform-set 1
 security acl 3001
 ike-profile branchB
#
ipsec policy test 1 isakmp template branchA
#
ipsec policy test 2 isakmp template branchB
#
ike dpd interval 10 on-deman
#
ike profile branchA
 keychain branchA
 exchange-mode aggressive
 local-identity fqdn headquarters
 match remote identity fqdn branchA
#
ike profile branchB
 keychain branchB
 exchange-mode aggressive
 local-identity fqdn headquarters
 match remote identity fqdn branchB
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain branchA
 match local address 1.1.1.2
 pre-shared-key hostname branchA key cipher $c$3$nng95cm/zlG3ghvIRim5saZ3bMEhoJD+Ow==
#
ike keychain branchB
 match local address 1.1.1.2
 pre-shared-key hostname branchB key cipher $c$3$Rl2okdkTYNBEYWd32X25LOWYkYo5YCcrgw=
=
#
```

分支A：

```
#
nqa entry admin test
 type icmp-echo
  destination ip 192.168.1.1
  frequency 5000
  history-record enable
  history-record number 10
  probe count 10
  probe timeout 500
  source ip 192.168.2.1
#
nqa entry admin test1
 type icmp-echo
  destination ip 192.168.3.1
  frequency 5000
  history-record enable
  history-record number 10
  probe count 10
  probe timeout 500
  source ip 192.168.2.1
#
 nqa schedule admin test start-time now lifetime forever
 nqa schedule admin test1 start-time now lifetime forever
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 2.2.2.2 255.255.255.252
 nat outbound 3001
 ipsec apply policy 1
#
 ip route-static 0.0.0.0 0 2.2.2.1
#
acl advanced 3000
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
 rule 5 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
#
acl advanced 3001
 rule 0 deny ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
 rule 5 deny ip source 192.168.2.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
 rule 100 permit ip
#
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3000
 remote-address 1.1.1.2
 ike-profile 1
#
ike dpd interval 10 on-demand
#
ike profile 1
 keychain 1
 exchange-mode aggressive
 local-identity fqdn branchA
 match remote identity fqdn headquarters
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain 1
 pre-shared-key address 1.1.1.2 255.255.255.0 key cipher
$c$3$5QlYyBFEZTju/oTPut9zgP5JNpmVleBIbA==
#
```

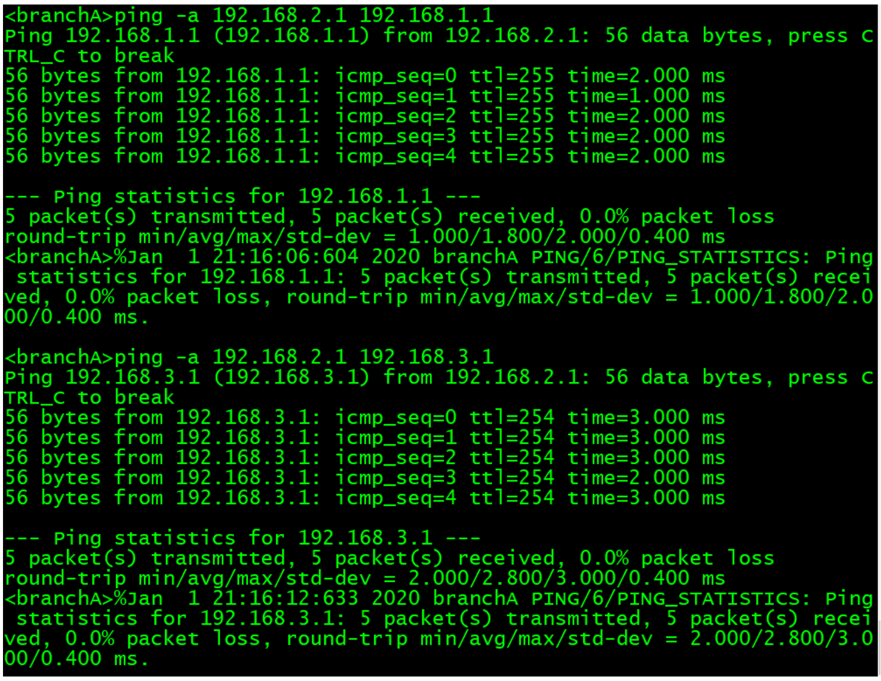
分支B：

```
#
nqa entry admin test
 type icmp-echo
  destination ip 192.168.1.1
  frequency 5000
  history-record enable
  history-record number 10
  probe count 10
  probe timeout 500
  source ip 192.168.3.1
#
```

```
nqa entry admin test1
 type icmp-echo
  destination ip 192.168.2.1
  frequency 5000
  history-record enable
  history-record number 10
  probe count 10
  probe timeout 500
  source ip 192.168.3.1
#
 nqa schedule admin test start-time now lifetime forever
 nqa schedule admin test1 start-time now lifetime forever
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 3.3.3.2 255.255.255.252
 nat outbound 3001
 ipsec apply policy 1
#
 ip route-static 0.0.0.0 0 3.3.3.1
#
acl advanced 3000
 rule 0 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
 rule 5 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
#
acl advanced 3001
 rule 0 deny ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
 rule 5 deny ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
 rule 100 permit ip
#
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3000
 remote-address 1.1.1.2
 ike-profile 1
#
ike dpd interval 10 on-demand
#
ike profile 1
 keychain 1
 exchange-mode aggressive
 local-identity fqdn branchB
 match remote identity fqdn headquarters
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain 1
 pre-shared-key address 1.1.1.2 255.255.255.0 key cipher
$c$3$5QlYyBFEZTju/oTPut9zgP5JNpmVleBIbA==
#
```

4、测试

分支A侧可以ping通总部和分支B



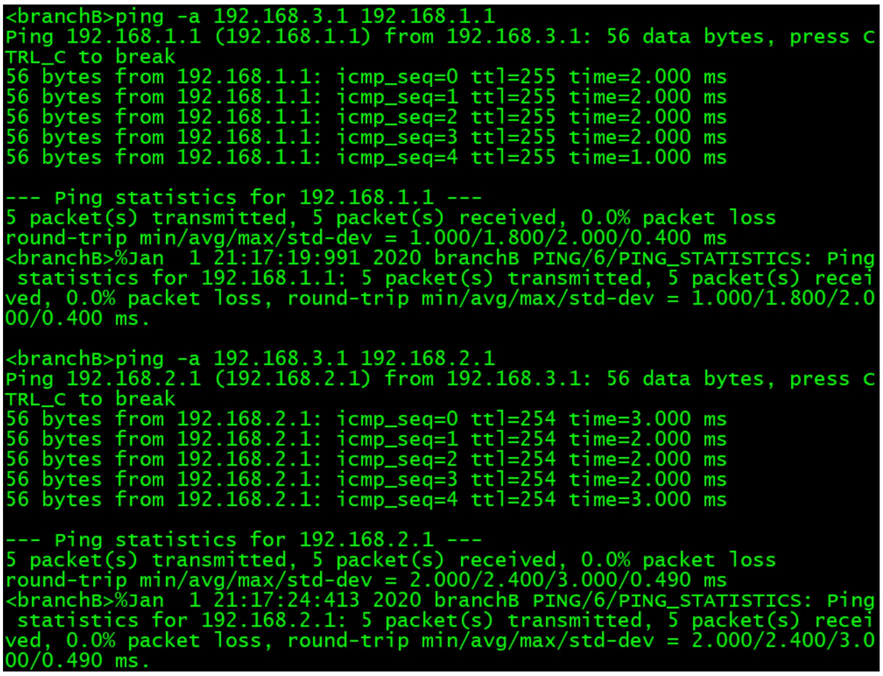
```
<branchA>ping -a 192.168.2.1 192.168.1.1
Ping 192.168.1.1 (192.168.1.1) from 192.168.2.1: 56 data bytes, press C
TRL_C to break
56 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=2.000 ms
56 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for 192.168.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.800/2.000/0.400 ms
<branchA>%Jan  1 21:16:06:604 2020 branchA PING/6/PING_STATISTICS: Ping
 statistics for 192.168.1.1: 5 packet(s) transmitted, 5 packet(s) recei
ved, 0.0% packet loss, round-trip min/avg/max/std-dev = 1.000/1.800/2.0
00/0.400 ms.

<branchA>ping -a 192.168.2.1 192.168.3.1
Ping 192.168.3.1 (192.168.3.1) from 192.168.2.1: 56 data bytes, press C
TRL_C to break
56 bytes from 192.168.3.1: icmp_seq=0 ttl=254 time=3.000 ms
56 bytes from 192.168.3.1: icmp_seq=1 ttl=254 time=3.000 ms
56 bytes from 192.168.3.1: icmp_seq=2 ttl=254 time=3.000 ms
56 bytes from 192.168.3.1: icmp_seq=3 ttl=254 time=2.000 ms
56 bytes from 192.168.3.1: icmp_seq=4 ttl=254 time=3.000 ms

--- Ping statistics for 192.168.3.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.000/2.800/3.000/0.400 ms
<branchA>%Jan  1 21:16:12:633 2020 branchA PING/6/PING_STATISTICS: Ping
 statistics for 192.168.3.1: 5 packet(s) transmitted, 5 packet(s) recei
ved, 0.0% packet loss, round-trip min/avg/max/std-dev = 2.000/2.800/3.0
00/0.400 ms.
```

分支B侧可以ping通总部和分支A



```
<branchB>ping -a 192.168.3.1 192.168.1.1
Ping 192.168.1.1 (192.168.1.1) from 192.168.3.1: 56 data bytes, press C
TRL_C to break
56 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=2.000 ms
56 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 192.168.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.800/2.000/0.400 ms
<branchB>%Jan  1 21:17:19:991 2020 branchB PING/6/PING_STATISTICS: Ping
 statistics for 192.168.1.1: 5 packet(s) transmitted, 5 packet(s) recei
ved, 0.0% packet loss, round-trip min/avg/max/std-dev = 1.000/1.800/2.0
00/0.400 ms.

<branchB>ping -a 192.168.3.1 192.168.2.1
Ping 192.168.2.1 (192.168.2.1) from 192.168.3.1: 56 data bytes, press C
TRL_C to break
56 bytes from 192.168.2.1: icmp_seq=0 ttl=254 time=3.000 ms
56 bytes from 192.168.2.1: icmp_seq=1 ttl=254 time=2.000 ms
56 bytes from 192.168.2.1: icmp_seq=2 ttl=254 time=2.000 ms
56 bytes from 192.168.2.1: icmp_seq=3 ttl=254 time=2.000 ms
56 bytes from 192.168.2.1: icmp_seq=4 ttl=254 time=3.000 ms

--- Ping statistics for 192.168.2.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.000/2.400/3.000/0.490 ms
<branchB>%Jan  1 21:17:24:413 2020 branchB PING/6/PING_STATISTICS: Ping
 statistics for 192.168.2.1: 5 packet(s) transmitted, 5 packet(s) recei
ved, 0.0% packet loss, round-trip min/avg/max/std-dev = 2.000/2.400/3.0
00/0.490 ms.
```

在总部侧查看ike sa 和ipsec sa

```
<Headquarters>dis ike sa
  Connection-ID  Remote            Flag       DOI
-------------------------------------------------------------------
  1            2.2.2.2          RD         IPsec
  2            3.3.3.2          RD         IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
<Headquarters>dis ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------

  -----------------------------
  IPsec policy: test
  Sequence number: 1
  Mode: Template
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
  Perfect Forward Secrecy:
  Inside VPN:
  Extended Sequence Numbers enable: N
  Traffic Flow Confidentiality enable: N
  Path MTU: 1444
  Tunnel:
      local  address: 1.1.1.2
      remote address: 2.2.2.2
  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: 2857585848 (0xaa534cb8)
    Connection ID: 4294967296
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843148/3404
    Max received sequence-number: 390
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

  [Outbound ESP SAs]
    SPI: 1462782990 (0x57304c0e)
    Connection ID: 4294967298
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843148/3404
    Max sent sequence-number: 390
    UDP encapsulation used for NAT traversal: N
    Status: Active

-----------------------------
IPsec policy: test
Sequence number: 1
Mode: Template
-----------------------------
  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: 1.1.1.2
      remote address: 2.2.2.2
  Flow:
      sour addr: 192.168.3.0/255.255.255.0  port: 0  protocol: ip
      dest addr: 192.168.2.0/255.255.255.0  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 1741076224 (0x67c6b700)
    Connection ID: 4294967297
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843095/3404
    Max received sequence-number: 790
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active
  [Outbound ESP SAs]
    SPI: 1031673059 (0x3d7e14e3)
    Connection ID: 4294967299
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843095/3404
    Max sent sequence-number: 790
    UDP encapsulation used for NAT traversal: N
    Status: Active

-----------------------------
IPsec policy: test
Sequence number: 2
Mode: Template
-----------------------------
  Tunnel id: 2
  Encapsulation mode: tunnel
  Perfect Forward Secrecy:
  Inside VPN:
  Extended Sequence Numbers enable: N
  Traffic Flow Confidentiality enable: N
  Path MTU: 1444
  Tunnel:
      local  address: 1.1.1.2
      remote address: 3.3.3.2
  Flow:
      sour addr: 192.168.1.0/255.255.255.0  port: 0  protocol: ip
      dest addr: 192.168.3.0/255.255.255.0  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 3005711568 (0xb32784d0)
    Connection ID: 4294967300
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843148/3404
    Max received sequence-number: 390
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

  [Outbound ESP SAs]
    SPI: 2370986263 (0x8d526117)
    Connection ID: 4294967302
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843148/3404
    Max sent sequence-number: 390
    UDP encapsulation used for NAT traversal: N
    Status: Active

-----------------------------
IPsec policy: test
Sequence number: 2
Mode: Template
-----------------------------
  Tunnel id: 3
  Encapsulation mode: tunnel
  Perfect Forward Secrecy:
  Inside VPN:
  Extended Sequence Numbers enable: N
  Traffic Flow Confidentiality enable: N
  Path MTU: 1444
  Tunnel:
    local  address: 1.1.1.2
    remote address: 3.3.3.2
  Flow:
    sour addr: 192.168.2.0/255.255.255.0  port: 0  protocol: ip
    dest addr: 192.168.3.0/255.255.255.0  port: 0  protocol: ip

  [Inbound ESP SAs]
   SPI: 957577755 (0x39137a1b)
   Connection ID: 4294967301
   Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
   SA duration (kilobytes/sec): 1843200/3600
   SA remaining duration (kilobytes/sec): 1843095/3404
   Max received sequence-number: 790
   Anti-replay check enable: Y
   Anti-replay window size: 64
   UDP encapsulation used for NAT traversal: N
   Status: Active

  [Outbound ESP SAs]
   SPI: 2955794011 (0xb02dd65b)
   Connection ID: 4294967303
   Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
   SA duration (kilobytes/sec): 1843200/3600
   SA remaining duration (kilobytes/sec): 1843095/3404
   Max sent sequence-number: 790
   UDP encapsulation used for NAT traversal: N
   Status: Active
```

在分支A侧查看ike sa 和ipsec sa以及NQA相关信息

```
<branchA>dis ike sa
  Connection-ID   Remote              Flag        DOI
------------------------------------------------------------------
  1             1.1.1.2             RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
<branchA>dis ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------


 -----------------------------
 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: 2.2.2.2
    remote address: 1.1.1.2
  Flow:
    sour addr: 192.168.2.0/255.255.255.0  port: 0  protocol: ip
    dest addr: 192.168.3.0/255.255.255.0  port: 0  protocol: ip

  [Inbound ESP SAs]
   SPI: 1031673059 (0x3d7e14e3)
   Connection ID: 4294967296
   Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
   SA duration (kilobytes/sec): 1843200/3600
   SA remaining duration (kilobytes/sec): 1843082/3379
   Max received sequence-number: 890
   Anti-replay check enable: Y
   Anti-replay window size: 64
   UDP encapsulation used for NAT traversal: N
   Status: Active

  [Outbound ESP SAs]
   SPI: 1741076224 (0x67c6b700)
   Connection ID: 4294967299
   Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
   SA duration (kilobytes/sec): 1843200/3600
   SA remaining duration (kilobytes/sec): 1843082/3379
   Max sent sequence-number: 890
   UDP encapsulation used for NAT traversal: N
   Status: Active

 -----------------------------
 IPsec policy: 1
 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
  Path MTU: 1444
  Tunnel:
    local  address: 2.2.2.2
    remote address: 1.1.1.2
  Flow:
    sour addr: 192.168.2.0/255.255.255.0  port: 0  protocol: ip
    dest addr: 192.168.1.0/255.255.255.0  port: 0  protocol: ip

  [Inbound ESP SAs]
   SPI: 1462782990 (0x57304c0e)
   Connection ID: 4294967297
   Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
   SA duration (kilobytes/sec): 1843200/3600
   SA remaining duration (kilobytes/sec): 1843141/3379
   Max received sequence-number: 440
   Anti-replay check enable: Y
   Anti-replay window size: 64
   UDP encapsulation used for NAT traversal: N
   Status: Active

  [Outbound ESP SAs]
   SPI: 2857585848 (0xaa534cb8)
   Connection ID: 4294967298
   Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
   SA duration (kilobytes/sec): 1843200/3600
   SA remaining duration (kilobytes/sec): 1843141/3379
   Max sent sequence-number: 440
   UDP encapsulation used for NAT traversal: N
   Status: Active

<branchA>dis nqa result
NQA entry (admin admin, tag test) test results:
  Send operation times: 10            Receive response times: 10
  Min/Max/Average round trip time: 1/2/1
  Square-Sum of round trip time: 16
  Last succeeded probe time: 2020-01-01 20:59:48.9
 Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
NQA entry (admin admin, tag test1) test results:
  Send operation times: 10             Receive response times: 10
  Min/Max/Average round trip time: 2/7/2
  Square-Sum of round trip time: 85
  Last succeeded probe time: 2020-01-01 20:59:48.9
 Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0

<branchA>dis nqa statistics
NQA entry (admin admin, tag test) test statistics:
 NO. : 1
  Start time: 2020-01-01 20:55:03.8
  Life time: 313 seconds
  Send operation times: 630            Receive response times: 590
  Min/Max/Average round trip time: 1/3/1
  Square-Sum of round trip time: 867
 Extended results:
  Packet loss ratio: 6%
  Failures due to timeout: 0
  Failures due to internal error: 10
  Failures due to other errors: 30
NQA entry (admin admin, tag test1) test statistics:
 NO. : 1
  Start time: 2020-01-01 20:55:03.8
  Life time: 313 seconds
  Send operation times: 630            Receive response times: 590
  Min/Max/Average round trip time: 1/7/1
  Square-Sum of round trip time: 2477
 Extended results:
  Packet loss ratio: 6%
  Failures due to timeout: 0
  Failures due to internal error: 10
  Failures due to other errors: 30
<branchA>dis nqa history
NQA entry (admin admin, tag test) history records:
Index      Response     Status           Time
650        1            Succeeded        2020-01-01 21:00:23.9
649        2            Succeeded        2020-01-01 21:00:23.9
648        1            Succeeded        2020-01-01 21:00:23.9
647        1            Succeeded        2020-01-01 21:00:23.9
646        1            Succeeded        2020-01-01 21:00:23.8
645        1            Succeeded        2020-01-01 21:00:23.8
644        1            Succeeded        2020-01-01 21:00:23.8
643        1            Succeeded        2020-01-01 21:00:23.8
642        1            Succeeded        2020-01-01 21:00:23.8
641        1            Succeeded        2020-01-01 21:00:23.8
NQA entry (admin admin, tag test1) history records:
Index      Response     Status           Time
650        2            Succeeded        2020-01-01 21:00:23.9
649        2            Succeeded        2020-01-01 21:00:23.9
648        2            Succeeded        2020-01-01 21:00:23.9
647        2            Succeeded        2020-01-01 21:00:23.9
646        2            Succeeded        2020-01-01 21:00:23.9
645        2            Succeeded        2020-01-01 21:00:23.9
644        2            Succeeded        2020-01-01 21:00:23.9
643        3            Succeeded        2020-01-01 21:00:23.8
```

```
642       1          Succeeded       2020-01-01 21:00:23.8
641       2          Succeeded       2020-01-01 21:00:23.8
```

在分支B侧查看ike sa 和ipsec sa以及NQA相关信息

```
<branchB>dis ike sa
  Connection-ID   Remote                Flag         DOI
------------------------------------------------------------------
  1               1.1.1.2               RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
<branchB>dis ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------

 -----------------------------
 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: 3.3.3.2
    remote address: 1.1.1.2
  Flow:
    sour addr: 192.168.3.0/255.255.255.0  port: 0  protocol: ip
    dest addr: 192.168.2.0/255.255.255.0  port: 0  protocol: ip

  [Inbound ESP SAs]
   SPI: 2955794011 (0xb02dd65b)
   Connection ID: 4294967296
   Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
   SA duration (kilobytes/sec): 1843200/3600
   SA remaining duration (kilobytes/sec): 1843068/3353
   Max received sequence-number: 990
   Anti-replay check enable: Y
   Anti-replay window size: 64
   UDP encapsulation used for NAT traversal: N
   Status: Active

  [Outbound ESP SAs]
   SPI: 957577755 (0x39137a1b)
   Connection ID: 4294967299
   Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
   SA duration (kilobytes/sec): 1843200/3600
   SA remaining duration (kilobytes/sec): 1843068/3353
   Max sent sequence-number: 990
   UDP encapsulation used for NAT traversal: N
   Status: Active

 -----------------------------
 IPsec policy: 1
 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
  Path MTU: 1444
  Tunnel:
    local  address: 3.3.3.2
    remote address: 1.1.1.2
  Flow:
    sour addr: 192.168.3.0/255.255.255.0  port: 0  protocol: ip
    dest addr: 192.168.1.0/255.255.255.0  port: 0  protocol: ip

  [Inbound ESP SAs]
   SPI: 2370986263 (0x8d526117)
   Connection ID: 4294967297
   Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
   SA duration (kilobytes/sec): 1843200/3600
   SA remaining duration (kilobytes/sec): 1843134/3353
   Max received sequence-number: 490
   Anti-replay check enable: Y
   Anti-replay window size: 64
   UDP encapsulation used for NAT traversal: N
   Status: Active

  [Outbound ESP SAs]
   SPI: 3005711568 (0xb32784d0)
   Connection ID: 4294967298
   Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
   SA duration (kilobytes/sec): 1843200/3600
   SA remaining duration (kilobytes/sec): 1843134/3353
   Max sent sequence-number: 490
   UDP encapsulation used for NAT traversal: N
   Status: Active

<branchB>dis nqa result
NQA entry (admin admin, tag test) test results:
  Send operation times: 10            Receive response times: 10
  Min/Max/Average round trip time: 1/2/1
  Square-Sum of round trip time: 13
  Last succeeded probe time: 2020-01-01 21:00:34.3
 Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
NQA entry (admin admin, tag test1) test results:
  Send operation times: 10            Receive response times: 10
  Min/Max/Average round trip time: 1/2/1
  Square-Sum of round trip time: 37
  Last succeeded probe time: 2020-01-01 21:00:34.3
 Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0

<branchB>dis nqa statistics
NQA entry (admin admin, tag test) test statistics:
 NO. : 1
  Start time: 2020-01-01 20:55:09.3
  Life time: 334 seconds
  Send operation times: 670           Receive response times: 640
  Min/Max/Average round trip time: 1/3/1
  Square-Sum of round trip time: 917
 Extended results:
  Packet loss ratio: 4%
  Failures due to timeout: 0
  Failures due to internal error: 10
  Failures due to other errors: 20
NQA entry (admin admin, tag test1) test statistics:
 NO. : 1
  Start time: 2020-01-01 20:55:09.3
  Life time: 334 seconds
  Send operation times: 670            Receive response times: 640
  Min/Max/Average round trip time: 1/4/1
  Square-Sum of round trip time: 2551
 Extended results:
  Packet loss ratio: 4%
  Failures due to timeout: 0
  Failures due to internal error: 10
  Failures due to other errors: 20

<branchB>dis nqa history
NQA entry (admin admin, tag test) history records:
Index      Response     Status           Time
690        1            Succeeded        2020-01-01 21:00:49.3
689        2            Succeeded        2020-01-01 21:00:49.3
688        1            Succeeded        2020-01-01 21:00:49.3
687        1            Succeeded        2020-01-01 21:00:49.3
686        1            Succeeded        2020-01-01 21:00:49.3
685        1            Succeeded        2020-01-01 21:00:49.3
684        1            Succeeded        2020-01-01 21:00:49.3
683        1            Succeeded        2020-01-01 21:00:49.3
682        1            Succeeded        2020-01-01 21:00:49.3
681        2            Succeeded        2020-01-01 21:00:49.3
NQA entry (admin admin, tag test1) history records:
Index      Response     Status           Time
690        2            Succeeded        2020-01-01 21:00:49.3
689        2            Succeeded        2020-01-01 21:00:49.3
688        2            Succeeded        2020-01-01 21:00:49.3
687        2            Succeeded        2020-01-01 21:00:49.3
686        2            Succeeded        2020-01-01 21:00:49.3
685        3            Succeeded        2020-01-01 21:00:49.3
684        2            Succeeded        2020-01-01 21:00:49.3
683        1            Succeeded        2020-01-01 21:00:49.3
682        2            Succeeded        2020-01-01 21:00:49.3
681        2            Succeeded        2020-01-01 21:00:49.3
```

配置关键点

1、各分支通过NQA实现自动和总部建立好ipsec VPN隧道之后，想要实现分支间互访，还需要分支间互相访问一下，这样两个分支上才分别都有到达另外一个分支的ipsec sa，分支间才能互通。所以在两个分支上分贝配置了两个NQA，一个是自动去ping总部，还有另外一个自动去ping对应的分支。

2、为了防止总部重启，分支的无效的ipsec sa没有及时删除，从而导致总部重启之后，业务不通。需要在分支上配置DPD。

```
ike dpd interval 10 on-demand
```

实际测试只需要在两个分支上配置即可。