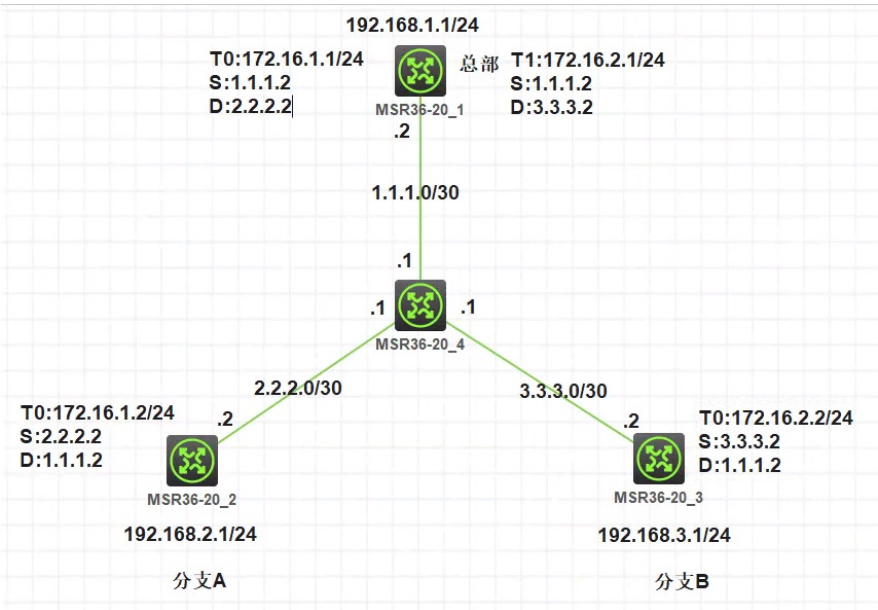
GRE over ipsec VPN multi-branch mutual access+automatical tunnel establishment

Routers 龚训杰 2020-12-15 Published

Network Topology



Demand

Establish GRE over ipsec vpn to realize intercommunication between each branch and the headquarters, and each branch can also access through the headquarters. The headquarters is a fixed IP address, the branch IP addresses are not fixed, and the branches A and B are unattended and the branches do not actively automatically access the business operations of the headquarters. Therefore, in order to prevent the branch equipment from being unable to actively establish tunnels after a power failure and restart, it is necessary to pass NQA to After the device is powered off and restarted, the tunnel establishment is automatically triggered.

Configuration Steps

HQ:

```
sysname Headquarters
#
interface LoopBack0
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 1.1.1.2 255.255.255.252
 nat outbound
 ipsec apply policy test
#
interface Tunnel0 mode gre
 description toBrabchA
 ip address 172.16.1.1 255.255.255.0
 source 1.1.1.2
 destination 2.2.2.2
```

```
#
interface Tunnel1 mode gre
 description toBrabchB
 ip address 172.16.2.11 255.255.255.0
 source 1.1.1.2
 destination 3.3.3.2
#
 ip route-static 0.0.0.0 0 1.1.1.1
 ip route-static 192.168.2.0 24 tunnel0
 ip route-static 192.168.3.0 24 tunnel1
#
acl advanced 3000
 description toBranchA
 rule 0 permit ip source 1.1.1.2 0.0.0.0 destination 2.2.2.2 0.0.0.0
#
acl advanced 3001
 description toBranchB
 rule 0 permit ip source 1.1.1.2 0.0.0.0 destination 3.3.3.2 0.0.0.0
#
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 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 simple 12345678
#
ike keychain branchB
 match local address 1.1.1.2
 pre-shared-key hostname branchB key simple 12345678
#
```

BranchA:

```
#
sysname branchA
#
nqa entry admin test
 type icmp-echo
  destination ip 1.1.1.2
  frequency 5000
  history-record enable
  history-record number 10
  probe count 10
  probe timeout 500
  source ip 2.2.2.2
#
 nqa schedule admin test start-time now lifetime forever
#
interface LoopBack0
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 2.2.2.2 255.255.255.252
 nat outbound
 ipsec apply policy 1
#
interface Tunnel0 mode gre
 ip address 172.16.1.2 255.255.255.0
 source 2.2.2.2
```

```
 destination 1.1.1.2
#
 ip route-static 0.0.0.0 0 2.2.2.1
 ip route-static 192.168.1.0 24 Tunnel0
 ip route-static 192.168.3.0 24 Tunnel0
#
acl advanced 3000
 rule 0 permit ip source 2.2.2.2 0.0.0.0 destination 1.1.1.2 0.0.0.0
#
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 simple 12345678
#
```

BranchB :

```
#
sysname branchB
#

nqa entry admin test
 type icmp-echo
  destination ip 1.1.1.2
  frequency 5000
  history-record enable
  history-record number 10
```

```
 probe count 10
 probe timeout 500
 source ip 3.3.3.2
#
 nqa schedule admin test start-time now lifetime forever
#
interface LoopBack0
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 3.3.3.2 255.255.255.252
 nat outbound
 ipsec apply policy 1
#
interface Tunnel0 mode gre
 ip address 172.16.1.3 255.255.255.0
 source 3.3.3.2
 destination 1.1.1.2
#
 ip route-static 0.0.0.0 0 3.3.3.
 ip route-static 192.168.1.0 24 Tunnel0

 ip route-static 192.168.2.0 24 Tunnel0
#
acl advanced 3000
 rule 0 permit ip source 3.3.3.2 0.0.0.0 destination 1.1.1.2 0.0.0.0
#
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 simple 12345678
```

Key Configuration

```
interface GigabitEthernet0/0
  port link-mode route
  ip address 1.1.1.2 255.255.255.252
//GRE packets will not be NATed, so there is no need for deny ipsec in the NAT area of interest.
  nat outbound
  ipsec apply policy test
```