# 分支单外网链路与总部双外网链路形成IPSEC VPN主备隧道配置方法

目录

# 1 配置需求及说明

## 1.1 适用的产品系列

本案例适用于软件平台为Comware V7系列防火墙：F100-X-G2、F1000-X-G2、F100-X-WiNet、F1000-AK、F10X0等。

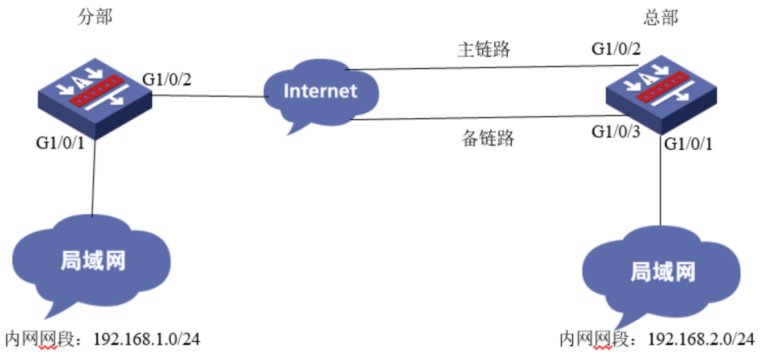
*注：本案例分支是F100-C-G2的Version 7.1.064, Release 9510P08版本，总部是F1000-C-G2的Version 7.1.064, Release 9323P1801上进行配置和验证的。*

## 1.2 配置需求及实现的效果

某大型互联网企业在全国各地都有分支机构，为提高业务的可靠性需要分支单位与总部单位建立互为主备的IPSEC隧道，总部为双互联网出口、分支为单互联网出口；IP地址及接口规划如下表所示：

| 公司名称 | 外网接口 | 公网地址/掩码 | 公网网关 | 内网接口 | 内网地址/掩码 |
|---|---|---|---|---|---|
| 总部（主链路） | G1/0/2 | 198.76.28.34/30 | 198.76.28.33 | G1/0/1 | 192.168.2.0/24 |
| 总部（备链路） | G1/0/3 | 202.34.6.90/30 | 202.34.6.89 | | |
| 分部 | G1/0/2 | 40.88.9.6/30 | 40.88.9.5 | G1/0/1 | 192.168.1.0/24 |

# 2 组网图




# 3 配置步骤

## 3.1 两端防火墙上网配置

防火墙上网配置请参考“2.3.2 防火墙外网使用固定IP地址上网配置方法”及“2.3.1 防火墙外网使用拨号上网配置方法”进行配置，本文只针对IPSEC VPN配置进行介绍。

## 3.2 分部侧创建IPSEC安全提议

#加密类型设置为3des-cbc，认证类型设置为md5。

```
[H3C]ipsec transform-set 1
[H3C-ipsec-transform-set-1]esp      encryption-algorithm
3des-cbc
[H3C-ipsec-transform-set-1]esp  authentication-algorithm
md5
[H3C-ipsec-transform-set-1]quit
```

注：IPSEC安全提议只需要创建一个，两条隧道都可以调用此IPSEC安全提议；

## 3.3 分部侧创建IKE安全提议

#IKE安全提议默认的认证类型为sha1，加密类型为DES-CBC，DH组为

DH1，所以不需要配置也存在这些参数。

```
[H3C]ike proposal 1
[H3C-ike-proposal-1]quit
```

## 3.4 分部侧创建IKE安全密钥

#创建两条IKE密钥，地址分别填写总部主链路地址与备链路地址，密码设置为123456。

```
[H3C]ike keychain 1
[H3C-ike-keychain-1]pre-shared-key address 198.76.28.34
255.255.255.255 key simple 123456
[H3C-ike-keychain-1]quit
[H3C]ike keychain 2
[H3C-ike-keychain-2]pre-shared-key address 202.34.6.90
255.255.255.255 key simple 123456
[H3C-ike-keychain-2]quit
```

## 3.5 分部侧创建IKE安全框架

#创建IKE安全框架，协商模式调整为野蛮模式。本端身份识别为a，总部身份识别为b，并指定总部主备链路的IP地址。

```
[H3C]ike identity fqdn a
[H3C]ike profile 1
[H3C-ike-profile-1]keychain 1
[H3C-ike-profile-1]exchange-mode aggressive
[H3C-ike-profile-1]local-identity fqdn a
[H3C-ike-profile-1]match remote identity address
198.76.28.34
[H3C-ike-profile-1]match remote identity fqdn b
[H3C-ike-profile-1]proposal 1
```

```
[H3C-ike-profile-1]quit
[H3C]ike profile 2
[H3C-ike-profile-2]keychain 2
[H3C-ike-profile-2]exchange-mode aggressive
[H3C-ike-profile-2]local-identity fqdn a
[H3C-ike-profile-2]match remote identity address
202.34.6.90
[H3C-ike-profile-2]match remote identity fqdn b
[H3C-ike-profile-2]proposal 1
[H3C-ike-profile-2]quit
```

## 3.6 分部侧创建IPSEC安全框架

```
[H3C]ipsec profile 1 isakmp
[H3C-ipsec-profile-isakmp-1]transform-set 1
[H3C-ipsec-profile-isakmp-1]ike-profile 1
[H3C-ipsec-profile-isakmp-1]quit
[H3C]ipsec profile 2 isakmp
[H3C-ipsec-profile-isakmp-2]transform-set 1
[H3C-ipsec-profile-isakmp-2]ike-profile 2
[H3C-ipsec-profile-isakmp-2]quit
```

## 3.7 分部侧创建IPSEC隧道

#创建IPsec隧道的接口Tunnel1并配置IPsec安全框架引用名称为1的IKE profile。

```
[H3C]interface Tunnel1 mode ipsec
[H3C-Tunnel1] ip address 8.8.8.8 255.255.255.0
[H3C-Tunnel1] source 40.88.9.6
```

```
[H3C-Tunnel1] destination 198.76.28.34
[H3C-Tunnel1] tunnel protection ipsec profile 1
[H3C-Tunnel1]quit
```

#创建IPsec隧道的接口Tunnel2并配置IPsec安全框架引用名称为2的IKE profile。

```
[H3C]interface Tunnel2 mode ipsec
[H3C-Tunnel2] ip address 9.9.9.9 255.255.255.0
[H3C-Tunnel2] source 40.88.9.6
[H3C-Tunnel2] destination 202.34.6.90
[H3C-Tunnel2] tunnel protection ipsec profile 2
[H3C-Tunnel2]quit
```

## 3.8 分部侧配置到总部内部网段的路由

#因为需要tunnel1为主隧道，因此到tunnel1路由的优先级要高于tunnel2路由优先级。

```
[H3C]ip route-static 192.168.2.0 24 Tunnel1
[H3C]ip route-static 192.168.2.0 24 Tunnel2 preference
70
```

## 3.9 保存配置

[H3C]save force

## 3.10 总部侧创建IPSEC安全提议

#加密类型设置为3des-cbc，认证类型设置为md5。

```
[H3C]ipsec transform-set 1
[H3C-ipsec-transform-set-1]esp encryption-algorithm
3des-cbc
[H3C-ipsec-transform-set-1]esp authentication-algorithm
```

```
md5
[H3C-ipsec-transform-set-1]quit
```

注：IPSEC安全提议只需要创建一个，两条隧道都可以调用此IPSEC安全提议；

## 3.11 总部侧创建IKE安全提议

#IKE安全提议默认的认证类型为sha1，加密类型为DES-CBC，DH组为DH1，所以不需要配置也存在这些参数。

```
[H3C]ike proposal 1
[H3C-ike-proposal-1]quit
```

## 3.12 总部侧创建IKE安全密钥

#创建两条IKE密钥，地址填写分部侧IP地址，密码设置为123456。

```
[H3C]ike keychain 1
[H3C-ike-keychain-1]pre-shared-key   address   40.88.9.6
255.255.255.255 key simple 123456
[H3C-ike-keychain-1]quit
[H3C]ike keychain 2
[H3C-ike-keychain-2]pre-shared-key   address   40.88.9.6
255.255.255.255 key simple 123456
[H3C-ike-keychain-2]quit
```

## 3.13 总部侧创建IKE安全框架

#创建IKE安全框架，协商模式调整为野蛮模式。本端身份识别为b，分部身份识别为a。

```
[H3C]ike identity fqdn b
[H3C]ike profile 1
[H3C-ike-profile-1]keychain 1
```

```
[H3C-ike-profile-1]exchange-mode aggressive
[H3C-ike-profile-1]local-identity fqdn b
[H3C-ike-profile-1]match remote identity fqdn a
[H3C-ike-profile-1]proposal 1
[H3C-ike-profile-1]quit
[H3C]ike profile 2
[H3C-ike-profile-2]keychain 2
[H3C-ike-profile-2]exchange-mode aggressive
[H3C-ike-profile-2]local-identity fqdn b
[H3C-ike-profile-2]match remote identity fqdn a
[H3C-ike-profile-2]proposal 1
[H3C-ike-profile-2]quit
```

## 3.14 分部侧创建IPSEC安全框架

```
[H3C]ipsec profile 1 isakmp
[H3C-ipsec-profile-isakmp-1]transform-set 1
[H3C-ipsec-profile-isakmp-1]ike-profile 1
[H3C-ipsec-profile-isakmp-1]quit
[H3C]ipsec profile 2 isakmp
[H3C-ipsec-profile-isakmp-2]transform-set 1
[H3C-ipsec-profile-isakmp-2]ike-profile 2
[H3C-ipsec-profile-isakmp-2]quit
```

## 3.15 分部侧创建IPSEC隧道

#创建IPsec隧道的接口Tunnel1并配置IPsec安全框架引用名称为1的IKE profile。

```
[H3C]interface Tunnel1 mode ipsec
```

```
[H3C-Tunnel1] ip address 8.8.8.9 255.255.255.0
[H3C-Tunnel1] source 198.76.28.34
[H3C-Tunnel1] destination 40.88.9.6
[H3C-Tunnel1] tunnel protection ipsec profile 1
[H3C-Tunnel1]quit
```

#创建IPsec隧道的接口Tunnel2并配置IPsec安全框架引用名称为2的IKE profile。

```
[H3C]interface Tunnel2 mode ipsec
[H3C-Tunnel2] ip address 9.9.9.10 255.255.255.0
[H3C-Tunnel2] source 202.34.6.90
[H3C-Tunnel2] destination 40.88.9.6
[H3C-Tunnel2] tunnel protection ipsec profile 2
[H3C-Tunnel2]quit
```

## 3.16 总部侧配置到分部内部网段的路由

#因为需要tunnel1为主隧道，因此到tunnel1路由的优先级要高于tunnel2路由优先级。

```
[H3C]ip route-static 192.168.1.0 24 Tunnel1
[H3C]ip route-static 192.168.1.0 24 Tunnel2 preference 70
```

## 3.17 保存配置

[H3C]save force

## 3.18 隧道验证

#分部通过命令行查看display ike sa可以看到隧道状态为RD状态表示ike建立完成。

```
<FWA>dis ike sa
   Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
   219             198.76.28.34          RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

分支通过display ipsec sa可以看到IPSEC SA基本状态。

```
<FWA>display ipsec sa
-------------------------------
Interface: Tunnel1
-------------------------------

  -------------------------------
  IPsec profile: 1
  Mode: ISAKMP
  -------------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Path MTU: 1388
    Tunnel:
        local  address: 40.88.9.6
        remote address: 198.76.28.34
    Flow:
        sour addr: 0.0.0.0/0.0.0.0  port: 0  protocol: ip
        dest addr: 0.0.0.0/0.0.0.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 2493522958 (0x94a0240e)
      Connection ID: 554050781185
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843198/1072
      Max received sequence-number: 19
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 3465718125 (0xce92a96d)
      Connection ID: 4294967298
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843198/1072
      Max sent sequence-number: 19
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

#总部通过命令行查看display ike sa可以看到隧道状态为RD状态表示ike建立完成。

```
<FWB>dis ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    18              40.88.9.6             RD           IPsec
    49              40.88.9.6             Unknown      IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

#总部通过display ipsec sa可以看到IPSEC SA基本状态。

```
<FWB>display ipsec sa
-------------------------------
Interface: Tunnel1
-------------------------------

  -----------------------------
  IPsec profile: 1
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Path MTU: 1388
    Tunnel:
        local  address: 198.76.28.34
        remote address: 40.88.9.6
    Flow:
        sour addr: 0.0.0.0/0.0.0.0  port: 0  protocol: ip
        dest addr: 0.0.0.0/0.0.0.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 3465718125 (0xce92a96d)
      Connection ID: 81604378624
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843198/969
      Max received sequence-number: 19
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 2493522958 (0x94a0240e)
      Connection ID: 4294967298
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843198/969
      Max sent sequence-number: 19
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

测试主隧道链路中断后VPN切换情况：将总部侧主链路接口shutdown；备SA备激活；

```
<FWA>dis ike sa
   Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
   847             202.34.6.90           RD           IPsec
   843             198.76.28.34          RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
<FWA>
<FWA>ping 192.168.2.1
Ping 192.168.2.1 (192.168.2.1): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.2.1: icmp_seq=0 ttl=255 time=0.636 ms
56 bytes from 192.168.2.1: icmp_seq=1 ttl=255 time=0.277 ms
56 bytes from 192.168.2.1: icmp_seq=2 ttl=255 time=0.231 ms
56 bytes from 192.168.2.1: icmp_seq=3 ttl=255 time=0.252 ms
56 bytes from 192.168.2.1: icmp_seq=4 ttl=255 time=0.253 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 = 0.231/0.330/0.636/0.154 ms
```

```
[FWA]display ipsec sa
-------------------------------
Interface: Tunnel2
-------------------------------

  -------------------------------
  IPsec profile: 2
  Mode: ISAKMP
  -------------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Path MTU: 1388
    Tunnel:
        local  address: 40.88.9.6
        remote address: 202.34.6.90
    Flow:
        sour addr: 0.0.0.0/0.0.0.0  port: 0  protocol: ip
        dest addr: 0.0.0.0/0.0.0.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 1871292357 (0x6f89a7c5)
      Connection ID: 1078036791296
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3503
      Max received sequence-number: 5
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 3024392536 (0xb4449158)
      Connection ID: 562640715777
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3503
      Max sent sequence-number: 5
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

## 3.19 实验注意事项

1、Tunnel接口会自动探测目的地址是否可达，如果目的地址可达则路由生效，路由不可达目的地址不生效，所以tunnel无法额外绑定NQA探测；

## 3.20 设备完整配置

分部侧所有配置：

```
#
 security-zone intra-zone default permit
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
```

```
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 40.88.9.6 255.255.255.252
 nat outbound
#
interface Tunnel1 mode ipsec
 ip address 8.8.8.8 255.255.255.0
 source 40.88.9.6
 destination 198.76.28.34
 tunnel protection ipsec profile 1
#
interface Tunnel2 mode ipsec
 ip address 9.9.9.9 255.255.255.0
 source 40.88.9.6
 destination 202.34.6.90
 tunnel protection ipsec profile 2
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
#
security-zone name Untrust
import interface GigabitEthernet1/0/2
import interface Tunnel1
import interface Tunnel2
#
```

```
 ip route-static 0.0.0.0 0 40.88.9.5
 ip route-static 192.168.2.0 24 Tunnel1
 ip route-static 192.168.2.0 24 Tunnel2 preference 70
#
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec profile 1 isakmp
 transform-set 1
 ike-profile 1
#
ipsec profile 2 isakmp
 transform-set 1
 ike-profile 2
#
 ike identity fqdn a
#
ike profile 1
 keychain 1
 exchange-mode aggressive
 local-identity fqdn a
 match remote identity fqdn b
 match remote identity fqdn 198.76.28.34
#
ike profile 2
```

```
 keychain 2
 exchange-mode aggressive
 local-identity fqdn a
 match remote identity fqdn b
 match remote identity fqdn 202.34.6.90
#
ike keychain 1
 pre-shared-key  address  198.76.28.34  255.255.255.255
key cipher $c$3$wN167W6uzXxhCS6A8Sjo9QdYuSH7Sg==
#
ike keychain 2
 pre-shared-key address 202.34.6.90 255.255.255.255 key
cipher $c$3$JP8dZ8yofSfIp2+QTKJ4GHKP7zm1OQ==
#
security-policy ip
 rule 1 name test
  action pass
#
```

总部侧完整配置：

```
#
 security-zone intra-zone default permit
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
```

```
 ip address 198.76.28.34 255.255.255.252
 nat outbound
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 202.34.6.90 255.255.255.252
 nat outbound
#
interface Tunnel1 mode ipsec
 ip address 8.8.8.9 255.255.255.0
 source 198.76.28.34
 destination 40.88.9.6
 tunnel protection ipsec profile 1
#
interface Tunnel2 mode ipsec
 ip address 9.9.9.10 255.255.255.0
 source 202.34.6.90
 destination 40.88.9.6
 tunnel protection ipsec profile 2
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
#
security-zone name Untrust
 import interface GigabitEthernet1/0/2
 import interface GigabitEthernet1/0/3
 import interface Tunnel1
 import interface Tunnel2
#
 ip route-static 0.0.0.0 0 198.76.28.33
 ip route-static 0.0.0.0 0 202.34.6.89 preference 70
 ip route-static 192.168.1.0 24 Tunnel1
 ip route-static 192.168.1.0 24 Tunnel2 preference 70
#
```

```
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec profile 1 isakmp
 transform-set 1
 ike-profile 1
#
ipsec profile 2 isakmp
 transform-set 1
 ike-profile 2
#
 ike identity fqdn b
#
ike profile 1
 keychain 1
 exchange-mode aggressive
 local-identity fqdn b
 match remote identity fqdn a
#
ike profile 2
 keychain 2
 exchange-mode aggressive
 local-identity fqdn b
 match remote identity fqdn a
#
ike proposal 1
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
#
ike keychain 1
 pre-shared-key  address  40.88.9.6  255.255.255.255  key
cipher $c$3$SAPwMObhQ33lNY0doESDhauhIUIV8g==
```

```
#
ike keychain 2
 pre-shared-key address 40.88.9.6 255.255.255.255 key
cipher $c$3$8EV+zB3Yufk80dRI0OER0CAMon1O8w==
```