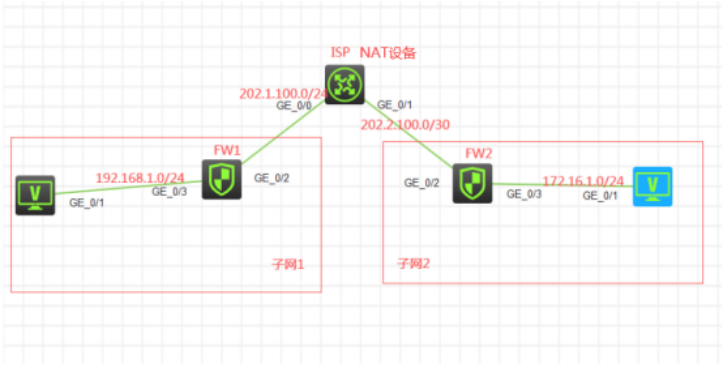
F1060 IPSEC典型组网配置案例（NAT穿越）

IPSec VPN　H3C模拟器　韦家宁　2020-02-28 发表

组网及说明



组网说明：

本案例采用H3C HCL模拟器的F1060防火墙来模拟IPSEC NAT穿越的典型组网配置。在网络拓扑图中存在子网1和子网2.为了保障子网1和子网2相互传输数据的安全性，因此需要在FW1与FW2采用建立IPSEC VPN隧道，由于FW1的出接口地址不固定且ISP为子网1的NAT设备，因此采用IKE野蛮模式。

配置步骤

1、按照网络拓扑图正确配置IP地址

2、ISP配置NAT

3、FW1与FW2的互联接口加入安全域，并放通域间策略

4、FW1与FW2建立IPSEC VPN隧道，采用IKE野蛮模式

配置关键点

ISP：

```
sys
System View: return to User View with Ctrl+Z.
[H3C]sysname ISP
[ISP]int gi 0/0
[ISP-GigabitEthernet0/0]des
[ISP-GigabitEthernet0/0]ip address 202.1.100.1 24
[ISP-GigabitEthernet0/0]dhcp server apply ip-pool 1
[ISP-GigabitEthernet0/0]quit
[ISP]acl basic 2000
[ISP-acl-ipv4-basic-2000]rule 0 permit source any
[ISP-acl-ipv4-basic-2000]quit
[ISP]int gi 0/1
[ISP-GigabitEthernet0/1]des
[ISP-GigabitEthernet0/1]ip address 202.2.100.1 30
[ISP-GigabitEthernet0/1]nat outbound 2000
[ISP-GigabitEthernet0/1]quit
[ISP]ip route-static 192.168.1.0 255.255.255.0 202.1.100.2
[ISP]ip route-static 172.16.1.0 255.255.255.0 202.2.100.2
[ISP]dhcp enable
[ISP]dhcp server ip-pool 1
[ISP-dhcp-pool-1]network 202.1.100.0 mask 255.255.255.0
[ISP-dhcp-pool-1]gateway-list 202.1.100.1
[ISP-dhcp-pool-1]quit
```

FW1：

```
sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW1
[FW1]int gi 1/0/3
[FW1-GigabitEthernet1/0/3]ip address 192.168.1.1 24
[FW1-GigabitEthernet1/0/3]quit
```

```
[FW1]int gi 1/0/2
[FW1-GigabitEthernet1/0/2]des
[FW1-GigabitEthernet1/0/2]ip address dhcp-alloc
[FW1-GigabitEthernet1/0/2]quit
[FW1]ip route-static 0.0.0.0 0.0.0.0 202.1.100.1
[FW1]security-zone name Trust
[FW1-security-zone-Trust]import interface GigabitEthernet 1/0/3
[FW1-security-zone-Trust]quit
[FW1]security-zone name Untrust
[FW1-security-zone-Untrust]import interface GigabitEthernet 1/0/2
[FW1-security-zone-Untrust]quit
[FW1]acl basic 2001
[FW1-acl-ipv4-basic-2001]rule 0 permit source any
[FW1-acl-ipv4-basic-2001]quit
[FW1]
[FW1]zone-pair security source trust destination untrust
[FW1-zone-pair-security-Trust-Untrust]packet-filter 2001
[FW1-zone-pair-security-Trust-Untrust]quit
[FW1]
[FW1]zone-pair security source untrust destination trust
[FW1-zone-pair-security-Untrust-Trust]packet-filter 2001
[FW1-zone-pair-security-Untrust-Trust]quit
[FW1]
[FW1]zone-pair security source trust destination local
[FW1-zone-pair-security-Trust-Local]packet-filter 2001
[FW1-zone-pair-security-Trust-Local]quit
[FW1]
[FW1]zone-pair security source local destination trust
[FW1-zone-pair-security-Local-Trust]packet-filter 2001
[FW1-zone-pair-security-Local-Trust]quit
[FW1]
[FW1]zone-pair security source untrust destination local
[FW1-zone-pair-security-Untrust-Local]packet-filter 2001
[FW1-zone-pair-security-Untrust-Local]quit
[FW1]
[FW1]zone-pair security source local destination untrust
[FW1-zone-pair-security-Local-Untrust]packet-filter 2001
[FW1-zone-pair-security-Local-Untrust]quit
```

FW1 IPSEC+IKE野蛮模式关键配置点：

```
[FW1]acl advanced 3000
[FW1-acl-ipv4-adv-3000]rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 172.16.1.0 0.0.0.25
5
[FW1-acl-ipv4-adv-3000]quit
[FW1]ike identity fqdn fw1
[FW1]ike keychain james
[FW1-ike-keychain-james]pre-shared-key address 202.2.100.2 255.255.255.252 key simple james
[FW1-ike-keychain-james]quit
[FW1]ike proposal 1
[FW1-ike-proposal-1]quit
[FW1]ike profile james
[FW1-ike-profile-james]keychain james
[FW1-ike-profile-james]proposal 1
[FW1-ike-profile-james]match remote identity address 202.2.100.2 255.255.255.252
[FW1-ike-profile-james]exchange-mode aggressive
[FW1-ike-profile-james]quit
[FW1]ipsec transform-set james
[FW1-ipsec-transform-set-james]protocol esp
[FW1-ipsec-transform-set-james]encapsulation-mode tunnel
[FW1-ipsec-transform-set-james]esp authentication-algorithm md5
[FW1-ipsec-transform-set-james]esp encryption-algorithm des-cbc
[FW1-ipsec-transform-set-james]quit
[FW1]ipsec policy james 1 isakmp
[FW1-ipsec-policy-isakmp-james-1]security acl 3000
```

```
[FW1-ipsec-policy-isakmp-james-1]transform-set james
[FW1-ipsec-policy-isakmp-james-1]ike-profile james
[FW1-ipsec-policy-isakmp-james-1]remote-address 202.2.100.2
[FW1-ipsec-policy-isakmp-james-1]quit
[FW1]int gi 1/0/2
[FW1-GigabitEthernet1/0/2]ipsec apply policy james
[FW1-GigabitEthernet1/0/2]quit
```

FW2：

```
sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW2
[FW2]int gi 1/0/3
[FW2-GigabitEthernet1/0/3]ip address 172.16.1.1 24
[FW2-GigabitEthernet1/0/3]quit
[FW2]int gi 1/0/2
[FW2-GigabitEthernet1/0/2]des
[FW2-GigabitEthernet1/0/2]ip address 202.2.100.2 30
[FW2-GigabitEthernet1/0/2]quit
[FW2]ip route-static 0.0.0.0 0.0.0.0 202.2.100.1
[FW2]security-zone name Untrust
[FW2-security-zone-Untrust]import interface GigabitEthernet 1/0/2
[FW2-security-zone-Untrust]quit
[FW2]security-zone name Trust
[FW2-security-zone-Trust]import interface GigabitEthernet 1/0/3
[FW2-security-zone-Trust]quit
[FW2]zone-pair security source trust destination untrust
[FW2-zone-pair-security-Trust-Untrust]packet-filter 2001
[FW2-zone-pair-security-Trust-Untrust]quit
[FW2]
[FW2]zone-pair security source untrust destination trust
[FW2-zone-pair-security-Untrust-Trust]packet-filter 2001
[FW2-zone-pair-security-Untrust-Trust]quit
[FW2]
[FW2]zone-pair security source trust destination local
[FW2-zone-pair-security-Trust-Local]packet-filter 2001
[FW2-zone-pair-security-Trust-Local]quit
[FW2]
[FW2]zone-pair security source local destination trust
[FW2-zone-pair-security-Local-Trust]packet-filter 2001
[FW2-zone-pair-security-Local-Trust]quit
[FW2]
[FW2]zone-pair security source untrust destination local
[FW2-zone-pair-security-Untrust-Local]packet-filter 2001
[FW2-zone-pair-security-Untrust-Local]quit
[FW2]
[FW2]zone-pair security source local destination untrust
[FW2-zone-pair-security-Local-Untrust]packet-filter 2001
[FW2-zone-pair-security-Local-Untrust]quit
```

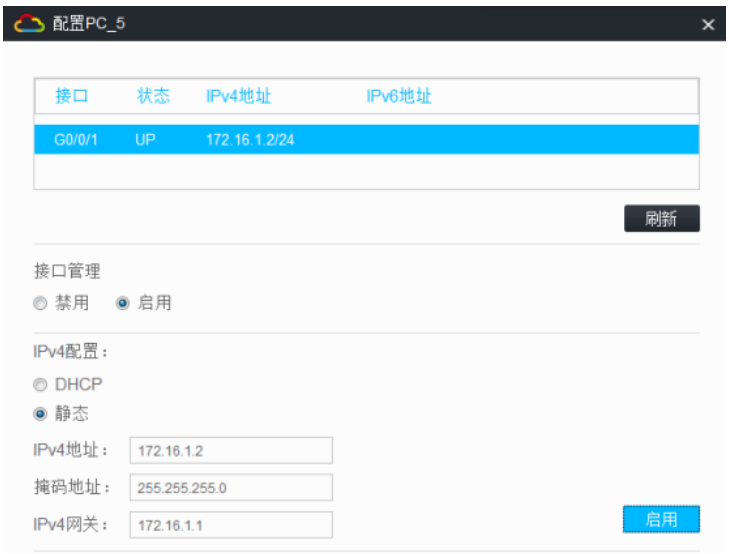
FW2 IPSEC+IKE野蛮模式关键配置点：

```
[FW2]acl advanced 3000
[FW2-acl-ipv4-adv-3000]rule 0 permit ip source 172.16.1.0 0.0.0.255 destination 192.168.1.0 0.0.0.25
5
[FW2-acl-ipv4-adv-3000]quit
[FW2]ike identity fqdn fw2
[FW2]ike proposal 1
[FW2-ike-proposal-1]quit
[FW2]ike keychain james
[FW2-ike-keychain-james]pre-shared-key hostname fw1 key simple james
[FW2-ike-keychain-james]quit
[FW2]ike profile james
[FW2-ike-profile-james]keychain james
[FW2-ike-profile-james]proposal 1
```

```
[FW2-ike-profile-james]match remote identity fqdn fw1
[FW2-ike-profile-james]exchange-mode aggressive
[FW2-ike-profile-james]quit
[FW2]ipsec transform-set james
[FW2-ipsec-transform-set-james]protocol esp
[FW2-ipsec-transform-set-james]encapsulation-mode tunnel
[FW2-ipsec-transform-set-james]esp authentication-algorithm md5
[FW2-ipsec-transform-set-james]esp encryption-algorithm des-cbc
[FW2-ipsec-transform-set-james]quit
[FW2]ipsec policy-template james 1
[FW2-ipsec-policy-template-james-1]security acl 3000
[FW2-ipsec-policy-template-james-1]transform-set james
[FW2-ipsec-policy-template-james-1]ike-profile james
[FW2-ipsec-policy-template-james-1]quit
[FW2]ipsec policy james 1 isakmp template james
[FW2]int gi 1/0/2
[FW2-GigabitEthernet1/0/2]ipsec apply policy james
[FW2-GigabitEthernet1/0/2]quit
```

测试：

物理机都填写IP地址：



PC之间可以相互PING通：

```
hcl_tszbme
F1060_1  F1060_2  PC_4  PC_5
<H3C>%Feb 28 08:32:28:579 2020 H3C SHELL/5/SHELL_LOGIN: Console logged in from con0.

<H3C>
<H3C>
<H3C>ping 172.16.1.2
Ping 172.16.1.2 (172.16.1.2): 56 data bytes, press CTRL_C to break
Request time out
56 bytes from 172.16.1.2: icmp_seq=1 ttl=253 time=4.000 ms
56 bytes from 172.16.1.2: icmp_seq=2 ttl=253 time=2.000 ms
56 bytes from 172.16.1.2: icmp_seq=3 ttl=253 time=3.000 ms
56 bytes from 172.16.1.2: icmp_seq=4 ttl=253 time=3.000 ms

--- Ping statistics for 172.16.1.2 ---
5 packet(s) transmitted, 4 packet(s) received, 20.0% packet loss
round-trip min/avg/max/std-dev = 2.000/3.000/4.000/0.707 ms
<H3C>%Feb 28 08:32:39:911 2020 H3C PING/6/PING_STATISTICS: Ping statistics for 172.16.1.2:
 5 packet(s) transmitted, 4 packet(s) received, 20.0% packet loss, round-trip min/avg/max/
std-dev = 2.000/3.000/4.000/0.707 ms.
```

```
hcl_tszbme
F1060_1  F1060_2  PC_4  PC_5
<H3C>%Feb 28 08:32:30:715 2020 H3C SHELL/5/SHELL_LOGIN: Console logged in from con0.

<H3C>ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=253 time=5.000 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=253 time=3.000 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=253 time=3.000 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=253 time=4.000 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=253 time=4.000 ms

--- Ping statistics for 192.168.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 3.000/3.800/5.000/0.748 ms
<H3C>%Feb 28 08:33:02:195 2020 H3C PING/6/PING_STATISTICS: Ping statistics for 192.168.1.2
: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/
std-dev = 3.000/3.800/5.000/0.748 ms.
```

查看FW1的IPSEC显示信息：

```
[FW1]dis ipsec tunnel
Tunnel ID: 0
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
SA's SPI:
    outbound:  22536596    (0x0157e194)   [ESP]
    inbound:   2245405840  (0x85d62c90)   [ESP]
Tunnel:
    local  address: 202.1.100.2
    remote address: 202.2.100.2
Flow:
        sour addr: 192.168.1.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 172.16.1.0/255.255.255.0  port: 0  protocol: ip
[FW1]
```

```
[FW1]dis ipsec policy
-------------------------------------------
IPsec Policy: james
Interface: GigabitEthernet1/0/2
-------------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: ISAKMP
  ----------------------------
  Traffic Flow Confidentiality: Disabled
  Security data flow: 3000
  Selector mode: standard
  Local address:
  Remote address: 202.2.100.2
  Transform set:  james
  IKE profile: james
  IKEv2 profile:
  smart-link policy:
  SA trigger mode: Traffic-based
  SA duration(time based): 3600 seconds
  SA duration(traffic based): 1843200 kilobytes
  SA soft-duration buffer(time based): --
  SA soft-duration buffer(traffic based): --
  SA idle time: --
[FW1]
```

```
[FW1]dis ipsec sa
-------------------------------
Interface: GigabitEthernet1/0/2
-------------------------------

  ----------------------------
  IPsec policy: james
  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: 202.1.100.2
        remote address: 202.2.100.2
    Flow:
        sour addr: 192.168.1.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 172.16.1.0/255.255.255.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 2245405840 (0x85d62c90)
      Connection ID: 4294967296
      Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3510
      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: 22536596 (0x0157e194)
      Connection ID: 4294967297
      Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3510
```

```
[FW1]dis ipsec transform-set
IPsec transform set: james
  State: complete
  Encapsulation mode: tunnel
  ESN: Disabled
  PFS:
  Transform: ESP
  ESP protocol:
    Integrity: MD5
    Encryption: DES-CBC

[FW1]
```

```
[FW1]dis ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    1               202.2.100.2           RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
[FW1]
```

查看FW1出接口配置及获取到的IP地址：

```
[FW1]dis int brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
GE1/0/0              DOWN DOWN     --
GE1/0/1              DOWN DOWN     192.168.0.1
GE1/0/2              UP   UP       202.1.100.2     <connect to ISP>
GE1/0/3              UP   UP       192.168.1.1
GE1/0/4              DOWN DOWN     --
GE1/0/5              DOWN DOWN     --
GE1/0/6              DOWN DOWN     --
GE1/0/7              DOWN DOWN     --
GE1/0/8              DOWN DOWN     --
GE1/0/9              DOWN DOWN     --
GE1/0/10             DOWN DOWN     --
GE1/0/11             DOWN DOWN     --
GE1/0/12             DOWN DOWN     --
GE1/0/13             DOWN DOWN     --
GE1/0/14             DOWN DOWN     --
GE1/0/15             DOWN DOWN     --
GE1/0/16             DOWN DOWN     --
GE1/0/17             DOWN DOWN     --
GE1/0/18             DOWN DOWN     --
[FW1]
```

```
[FW1]dis cu int gi 1/0/2
#
interface GigabitEthernet1/0/2
 port link-mode route
 description <connect to ISP>
 combo enable copper
 ip address dhcp-alloc
 ipsec apply policy james
#
return
[FW1]
```

查看ISP DHCP分配出去的地址：

```
<ISP>dis dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
202.1.100.2      0039-6535-662e-3462-  Feb 29 09:08:49 2020  Auto(C)
                 6431-2e30-3130-372d-
                 4745-312f-302f-32
<ISP>
```

查看FW2的IPSEC显示信息：

```
[FW2]dis ipsec tunnel
Tunnel ID: 0
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
SA's SPI:
    outbound:  2245405840  (0x85d62c90)   [ESP]
    inbound:   22536596    (0x0157e194)   [ESP]
Tunnel:
    local  address: 202.2.100.2
    remote address: 202.1.100.2
Flow:
        sour addr: 172.16.1.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 192.168.1.0/255.255.255.0  port: 0  protocol: ip
[FW2]
```

```
[FW2]dis ipsec policy
-------------------------------------------
IPsec Policy: james
Interface: GigabitEthernet1/0/2
-------------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: Template
  ----------------------------
  Policy template name: james
[FW2]
```

```
[FW2]dis ipsec policy-template
-------------------------------------------
IPsec Policy Template: james
-------------------------------------------

  ----------------------------
  Sequence number: 1
  ----------------------------
  Traffic Flow Confidentiality: Disabled
  Security data flow : 3000
  Selector mode: standard
  Local address:
  IKE profile: james
  IKEv2 profile:
  Remote address:
  Transform set: james
  IPsec SA local duration(time based): 3600 seconds
  IPsec SA local duration(traffic based): 1843200 kilobytes
  SA idle time: --
[FW2]
```

```
[FW2]dis ipsec transform-set
IPsec transform set: james
  State: complete
  Encapsulation mode: tunnel
  ESN: Disabled
  PFS:
  Transform: ESP
  ESP protocol:
    Integrity: MD5
    Encryption: DES-CBC

[FW2]
```

```
[FW2]dis ipsec sa
-------------------------------
Interface: GigabitEthernet1/0/2
-------------------------------

  ----------------------------
  IPsec policy: james
  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: 202.2.100.2
        remote address: 202.1.100.2
    Flow:
        sour addr: 172.16.1.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 192.168.1.0/255.255.255.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 22536596 (0x0157e194)
      Connection ID: 4294967296
      Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3323
      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: 2245405840 (0x85d62c90)
      Connection ID: 4294967297
      Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3323
```

```
[FW2] dis ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    1               202.1.100.2           RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
[FW2]
```

至此，F1060 IPSEC NAT穿越典型组网配置案例已完成！