

知 F1060 IPSEC+IKE预共享密钥典型组网配置案例

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+IKE预共享密钥的典型组网配置。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IKE预共享的方式建立IPSEC VPN隧道。

配置步骤

配置思路：

- 1、按照网络拓扑图正确配置IP地址
- 2、FW1与FW2的互联接口加入安全域，并放通域间策略
- 3、FW1与FW2建立IPSEC VPN隧道，采用IKE预共享的方式

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 30

[ISP-GigabitEthernet0/0]quit

[ISP]int gi 0/1

[ISP-GigabitEthernet0/1]des

[ISP-GigabitEthernet0/1]ip address 202.2.100.1 30

[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

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 202.1.100.2 30

[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]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预共享密钥 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 0.0.0.255
[FW1-acl-ipv4-adv-3000]quit
[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]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.

```
[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 Trust
[FW2-security-zone-Trust]import interface GigabitEthernet 1/0/3
[FW2-security-zone-Trust]quit
[FW2]security-zone name Untrust
[FW2-security-zone-Untrust]import interface GigabitEthernet 1/0/2
[FW2-security-zone-Untrust]quit
[FW2]acl basic 2001
[FW2-acl-ipv4-basic-2001]rule 0 permit source any
[FW2-acl-ipv4-basic-2001]quit
[FW2]
[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预共享密钥 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 0.0.0.255
5
[FW2-acl-ipv4-adv-3000]quit
[FW2]ike keychain james
[FW2-ike-keychain-james]pre-shared-key address 202.1.100.2 255.255.255.252 key simple james
[FW2-ike-keychain-james]quit
[FW2]ike proposal 1
[FW2-ike-proposal-1]quit
[FW2]ike profile james
[FW2-ike-profile-james]keychain james
[FW2-ike-profile-james]proposal 1
[FW2-ike-profile-james]match remote identity address 202.1.100.2 255.255.255.252
[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 james 1 isakmp
[FW2-ipsec-policy-isakmp-james-1]security acl 3000
[FW2-ipsec-policy-isakmp-james-1]ike-profile james
[FW2-ipsec-policy-isakmp-james-1]transform-set james
[FW2-ipsec-policy-isakmp-james-1]remote-address 202.1.100.2
[FW2-ipsec-policy-isakmp-james-1]quit
```

[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：

配置PC_4

接口	状态	IPv4地址	IPv6地址
G0/0/1	UP	192.168.1.2/24	

刷新

接口管理

☐ 禁用

☒ 启用

IPv4配置：

☐ DHCP

☒ 静态

IPv4地址：

192.168.1.2

掩码地址：

255.255.255.0

IPv4网关：

192.168.1.1

启用

配置PC_5

接口	状态	IPv4地址	IPv6地址
G0/0/1	UP	172.16.1.2/24	

刷新

接口管理

☐ 禁用

☒ 启用

IPv4配置：

☐ DHCP

☒ 静态

IPv4地址：

172.16.1.2

掩码地址：

255.255.255.0

IPv4网关：

172.16.1.1

启用

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_ts2bme
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: 3756757535 (0xdfb921f) [ESP]
  inbound: 4114820926 (0xf5432f3e) [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 date flow: 3000
Sequence mode: random
Local address:
Remote address: 202.1.100.2
Transform set: james
IKE profile: james
IPsec profile:
  next-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 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 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: 4114820926 (0xf5432f3e)
Connection ID: 4294967296
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3439
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: 3756757535 (0xdfb921f)
Connection ID: 4294967297
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3439
```

```

[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: 4114820926 (0xf5432f3e) [ESP]
inbound: 3756757535 (0xdfeb921f) [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
-----
Name: Policy1 James
Interface: GigabitEthernet1/0/2
-----
Sequence number: 1
Mode: ISAKMP
Traffic Flow Confidentiality: Disabled
Security data flow: 3600
Selection mode: standard
Local address:
Remote address: 202.1.100.2
Transform set: James
IKE profile: James
IKEv2 profile:
Smart-link policy:
SA trigger mode: Traffic-based
SA duration(time based): 1800 seconds
SA duration(traffic based): 1843200 kilobytes
SA soft-duration buffer(time based): --
SA soft-duration buffer(traffic based): --
SA idle timer: --
[FW2]

```

```

[FW2]dis ipsec transform-set
IPsec transform set: James
State: complete
Encapsulation mode: tunnel
ESP: Disabled
MD5:
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: 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: 202.2.100.2
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: 3756757535 (0xdfeb921f)
Connection ID: 4294967296
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3293
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: 4114820926 (0xf5432f3e)
Connection ID: 4294967297
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600

```

```

[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+IKE预共享密钥典型组网配置案例已完成！

