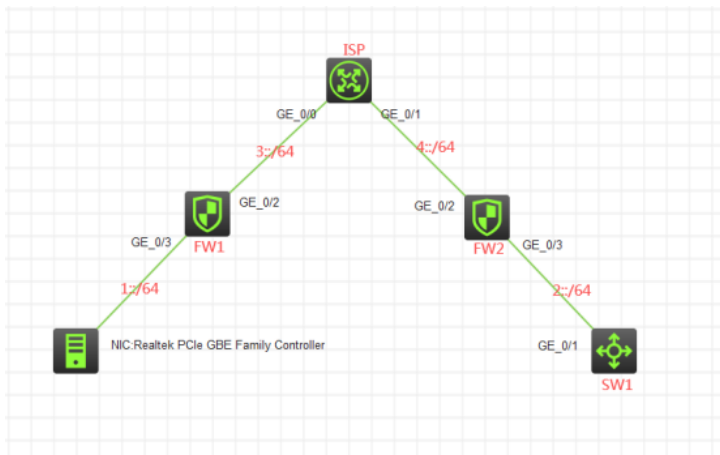


知 F1060 IPV6 IPSEC+野蛮模式典型组网配置案例

IPSec VPN 设备部署方式 H3C模拟器 韦家宁 2020-03-08 发表

组网及说明



组网说明:

本案例采用H3C HCL模拟器的F1060来模拟IPV6 IPSEC+IKE预共享密钥的典型组网配置。为了保障1::/64与2::/64之间传输数据的安全性，因此需要在FW1与FW2之间建立IPSEC VPN隧道，由于FW1的与上行的互联接口没有固定的IP地址，因此采用IPSEC野蛮模式的方式来进行组网。

配置步骤

- 1、按照网络拓扑图正确配置IP地址
- 2、FW1、FW2、ISP之间通过默认路由器及静态路由相互指向
- 3、FW1与FW2之间采用IPSEC野蛮的方式建立VPN隧道
- 4、ISP配置DHCPv6，为FW1的接入提供IPV6的地址分配

配置关键点

SW1:

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname SW1
[SW1]int gi 1/0/1
[SW1-GigabitEthernet1/0/1]port link-mode route
[SW1-GigabitEthernet1/0/1]des <connect to FW2>
[SW1-GigabitEthernet1/0/1]ipv6 address 2::2 64
[SW1-GigabitEthernet1/0/1]quit
[SW1]ipv6 route-static :: 0 2::1
```

ISP:

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname ISP
[ISP]ipv6 dhcp prefix-pool 1 prefix 3::/64 assign-len 64
[ISP]ipv6 dhcp pool 1
[ISP-dhcp6-pool-1]network 3::/64
[ISP-dhcp6-pool-1]gateway-list 3::2
[ISP-dhcp6-pool-1]prefix-pool 1 preferred-lifetime 86400 valid-lifetime 259200
[ISP-dhcp6-pool-1]quit
[ISP]int gi 0/0
[ISP-GigabitEthernet0/0]des <connect to FW1>
[ISP-GigabitEthernet0/0]ipv6 address 3::2 64
[ISP-GigabitEthernet0/0]ipv6 dhcp select server
[ISP-GigabitEthernet0/0]ipv6 dhcp server allow-hint preference 255 rapid-commit
[ISP-GigabitEthernet0/0]undo ipv6 nd ra halt
[ISP-GigabitEthernet0/0]ipv6 nd autoconfig managed-address-flag
[ISP-GigabitEthernet0/0]ipv6 nd autoconfig other-flag
[ISP-GigabitEthernet0/0]quit
[ISP]int gi 0/1
```

```
[ISP-GigabitEthernet0/1]des <connect to FW2>
[ISP-GigabitEthernet0/1]ipv6 address 4::2 64
[ISP-GigabitEthernet0/1]quit
[ISP]ipv6 route-static 1:: 64 3::1
[ISP]ipv6 route-static 2:: 64 4::1
[ISP]dhcp enable
```

FW2 :

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW2
[FW2]acl ipv6 basic 2001
[FW2-acl-ipv6-basic-2001]rule 0 permit source any
[FW2-acl-ipv6-basic-2001]quit
[FW2]zone-pair security source trust destination untrust
[FW2-zone-pair-security-Trust-Untrust]packet-filter ipv6 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 ipv6 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 ipv6 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 ipv6 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 ipv6 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 ipv6 2001
[FW2-zone-pair-security-Local-Untrust]quit
[FW2]
[FW2]zone-pair security source trust destination trust
[FW2-zone-pair-security-Trust-Trust]packet-filter ipv6 2001
[FW2-zone-pair-security-Trust-Trust]quit
[FW2]
[FW2]zone-pair security source untrust destination untrust
[FW2-zone-pair-security-Untrust-Untrust]packet-filter ipv6 2001
[FW2-zone-pair-security-Untrust-Untrust]quit
[FW2]int gi 1/0/3
[FW2-GigabitEthernet1/0/3]des <connect to SW1>
[FW2-GigabitEthernet1/0/3]ipv6 address 2::1 64
[FW2-GigabitEthernet1/0/3]quit
[FW2]int gi 1/0/2
[FW2-GigabitEthernet1/0/2]des <connect to ISP>
[FW2-GigabitEthernet1/0/2]ipv6 address 4::1 64
[FW2-GigabitEthernet1/0/2]quit
[FW2]ipv6 route-static :: 0 4::2
[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 IPV6 IPSEC野蛮模式关键配置点:

```
[FW2]acl ipv6 advanced 3000
[FW2-acl-ipv6-adv-3000]rule 0 permit ipv6 source 2:: 64 destination 1:: 64
```

```
[FW2-acl-ipv6-adv-3000]quit
[FW2]ike identity fqdn fw2
[FW2]ike keychain james
[FW2-ike-keychain-james]pre-shared-key hostname fw1 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 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 ipv6-policy-template james 1
[FW2-ipsec-ipv6-policy-template-james-1]security acl ipv6 3000
[FW2-ipsec-ipv6-policy-template-james-1]transform-set james
[FW2-ipsec-ipv6-policy-template-james-1]ike-profile james
[FW2-ipsec-ipv6-policy-template-james-1]quit
[FW2]ipsec ipv6-policy james 1 isakmp template james
[FW2]int gi 1/0/2
[FW2-GigabitEthernet1/0/2]ipsec apply ipv6-policy james
[FW2-GigabitEthernet1/0/2]quit
```

FW1 :

<H3C>sys

System View: return to User View with Ctrl+Z.

[H3C]sysname FW1

[FW1]acl ipv6 basic 2001

[FW1-acl-ipv6-basic-2001]rule 0 permit source any

[FW1-acl-ipv6-basic-2001]quit

[FW1]zone-pair security source trust destination untrust

[FW1-zone-pair-security-Trust-Untrust]packet-filter ipv6 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 ipv6 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 ipv6 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 ipv6 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 ipv6 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 ipv6 2001

[FW1-zone-pair-security-Local-Untrust]quit

[FW1]

[FW1]zone-pair security source trust destination trust

[FW1-zone-pair-security-Trust-Trust]packet-filter ipv6 2001

[FW1-zone-pair-security-Trust-Trust]quit

[FW1]

```

[FW1]zone-pair security source untrust destination untrust
[FW1-zone-pair-security-Untrust-Untrust]packet-filter ipv6 2001
[FW1-zone-pair-security-Untrust-Untrust]quit
[FW1]int gi 1/0/3
[FW1-GigabitEthernet1/0/3]ipv6 address 1::1 64
[FW1-GigabitEthernet1/0/3]quit
[FW1]int gi 1/0/2
[FW1-GigabitEthernet1/0/2]des <connect to ISP>
[FW1-GigabitEthernet1/0/2]ipv6 address dhcp-alloc
[FW1-GigabitEthernet1/0/2]quit
[FW1]ipv6 route-static :: 0 3::2
[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 IPV6 IPSEC+野蛮模式关键配置点:

```

[FW1]acl ipv6 advanced 3000
[FW1-acl-ipv6-adv-3000]rule 0 permit ipv6 source 1:: 64 destination 2:: 64
[FW1-acl-ipv6-adv-3000]quit
[FW1]ike identity fqdn fw1
[FW1-ike-keychain-james]pre-shared-key address ipv6 4::1 64 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 ipv6 4::1 64
[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 ipv6-policy james 1 isakmp
[FW1-ipsec-ipv6-policy-isakmp-james-1]security acl ipv6 3000
[FW1-ipsec-ipv6-policy-isakmp-james-1]ike-profile james
[FW1-ipsec-ipv6-policy-isakmp-james-1]transform-set james
[FW1-ipsec-ipv6-policy-isakmp-james-1]remote-address ipv6 4::1
[FW1-ipsec-ipv6-policy-isakmp-james-1]quit
[FW1]int gi 1/0/2
[FW1-GigabitEthernet1/0/2]ipsec apply ipv6-policy james
[FW1-GigabitEthernet1/0/2]quit

```

查看FW1获取到的IP地址:

```

[FW1]dis cu int gi 1/0/2
#
interface GigabitEthernet1/0/2
 port link-mode route
 description <connect to ISP>
 combo enable copper
 ipv6 address dhcp-alloc
 ipsec apply ipv6-policy james
#
return
[FW1]

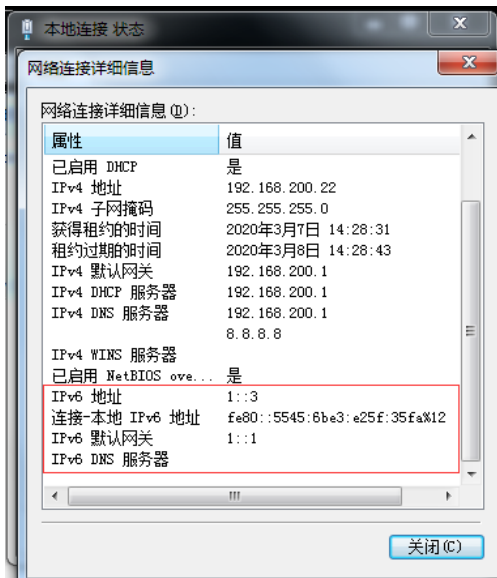
```

```
[FW1]dis ipv6 int brief
*down: administratively down
(s): spoofing
Interface                Physical Protocol IPv6 Address
GigabitEthernet1/0/0    down    down    Unassigned
GigabitEthernet1/0/1    down    down    Unassigned
GigabitEthernet1/0/2    up       up       3::1
GigabitEthernet1/0/3    up       up       1::1
GigabitEthernet1/0/4    down    down    Unassigned
GigabitEthernet1/0/5    down    down    Unassigned
GigabitEthernet1/0/6    down    down    Unassigned
GigabitEthernet1/0/7    down    down    Unassigned
GigabitEthernet1/0/8    down    down    Unassigned
GigabitEthernet1/0/9    down    down    Unassigned
GigabitEthernet1/0/10   down    down    Unassigned
GigabitEthernet1/0/11   down    down    Unassigned
GigabitEthernet1/0/12   down    down    Unassigned
GigabitEthernet1/0/13   down    down    Unassigned
GigabitEthernet1/0/14   down    down    Unassigned
GigabitEthernet1/0/15   down    down    Unassigned
GigabitEthernet1/0/16   down    down    Unassigned
GigabitEthernet1/0/17   down    down    Unassigned
GigabitEthernet1/0/18   down    down    Unassigned
GigabitEthernet1/0/19   down    down    Unassigned
GigabitEthernet1/0/20   down    down    Unassigned
GigabitEthernet1/0/21   down    down    Unassigned
GigabitEthernet1/0/22   down    down    Unassigned
GigabitEthernet1/0/23   down    down    Unassigned
[FW1]
```

在ISP查看分配出去的IPV6地址:

```
<ISP>dis ipv6 dhcp server ip-in-use
Pool: 1
IPv6 address                Type      Lease expiration
3::1                        Auto(C)   Apr  7 09:39:16 2020
<ISP>
```

物理机填写IPV6地址:



物理机能PING通SW1:

```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator.USER-20190510MA>ping 2::2

正在 Ping 2::2 具有 32 字节的数据:
来自 2::2 的回复: 时间=2ms
来自 2::2 的回复: 时间=2ms
来自 2::2 的回复: 时间=2ms
来自 2::2 的回复: 时间=2ms

2::2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 2ms, 最长 = 2ms, 平均 = 2ms

C:\Users\Administrator.USER-20190510MA>
```

SW1能PING通物理机:

```
hcl_ispnzh
Line con0 is available.
Press ENTER to get started.
<SW1>Mar  8 09:50:23:552 2020 SW1 SHELL/5/SHELL_LOGIN: Console logged in from con0.
<SW1>
<SW1>
<SW1>sys
System View: return to User View with Ctrl+Z.
[SW1]ping ipv6 1::3
Ping6(56 data bytes) 2::2 --> 1::3, press CTRL_C to break
56 bytes from 1::3, icmp_seq=0 hlim=126 time=3.000 ms
56 bytes from 1::3, icmp_seq=1 hlim=126 time=2.000 ms
56 bytes from 1::3, icmp_seq=2 hlim=126 time=4.000 ms
56 bytes from 1::3, icmp_seq=3 hlim=126 time=3.000 ms
56 bytes from 1::3, icmp_seq=4 hlim=126 time=3.000 ms

--- Ping6 statistics for 1::3 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.000/3.000/4.000/0.632 ms
[SW1]Mar  8 09:53:28:491 2020 SW1 PING/6/PING_STATISTICS: Ping6 statistics for 1::3: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/std-dev = 2.000/3.000/4.000/0.632 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: 1301447132 (0x4d9281dc) [ESP]
  inbound:  506056433 (0x1e29cef1) [ESP]
Tunnel:
  local address: 3::1
  remote address: 4::1
Flow:
  sour addr: 1::/64 port: 0 protocol: ipv6
  dest addr: 2::/64 port: 0 protocol: ipv6
[FW1]
```

```
[FW1]dis ipsec tunnel brief
-----
Tunn-id   Src Address   Dst Address   Inbound SPI   Outbound SPI   Status
-----
0         3::1         4::1         506056433    1301447132    Active
[FW1]
```

```
[FW1]dis ipsec ipv6-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: 4::1
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 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              4::1           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: 506056433 (0x1e29cef1) [ESP]
  inbound: 1301447132 (0x4d9281dc) [ESP]
Tunnel:
  local address: 4::1
  remote address: 3::1
Flow:
  sour addr: 2::/64 port: 0 protocol: ipv6
  dest addr: 1::/64 port: 0 protocol: ipv6
[FW2]
```

```
[FW2]dis ipsec tunnel brief
-----
Tunn-id  Src Address  Dst Address  Inbound SPI  Outbound SPI  Status
-----
0        4::1        3::1        1301447132  506056433    Active
[FW2]
```

```
[FW2]dis ipsec ipv6-policy
-----
IPsec Policy: james
Interface: GigabitEthernet1/0/2
-----

-----
Sequence number: 1
Mode: Template
-----

Policy template name: james
[FW2]
```

```
[FW2]dis ipsec ipv6-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 ike sa
-----
Connection-ID  Remote          Flag          DOI
-----
1              3::1           RD            IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
[FW2]
```

至此，F1060 IPV6 IPSEC+野蛮模式典型组网配置案例已完成!