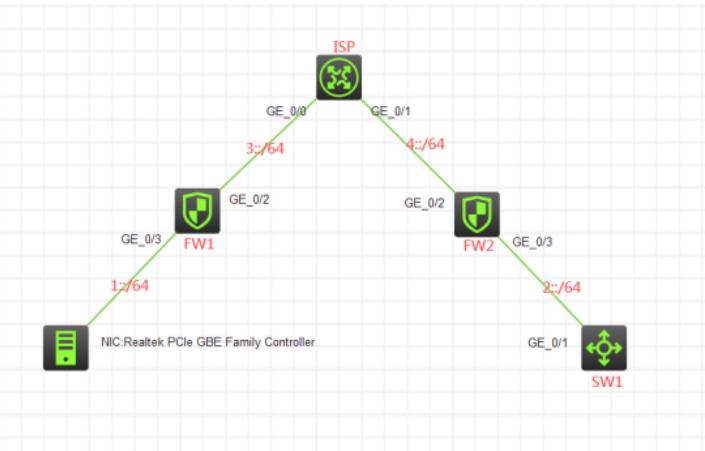


F1060 IPV6 IPSEC+IKE预共享密钥典型组网配置案例

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与FW2都有着固定的IP地址，因此采用IPSEC+IKE预共享密钥的方式来进行组网。

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+IKE预共享密钥的方式建立VPN隧道

配置关键点

ISP:
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname ISP
[ISP]int gi 0/0
[ISP-GigabitEthernet0/0]des <connect to FW1>
[ISP-GigabitEthernet0/0]ipv6 address 3::2 64
[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
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

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 3::1 64
[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+IKE预共享密钥关键配置点:

```
[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 keychain james
[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]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]transform-set james
[FW1-ipsec-ipv6-policy-isakmp-james-1]ike-profile 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
```

```
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
```

```

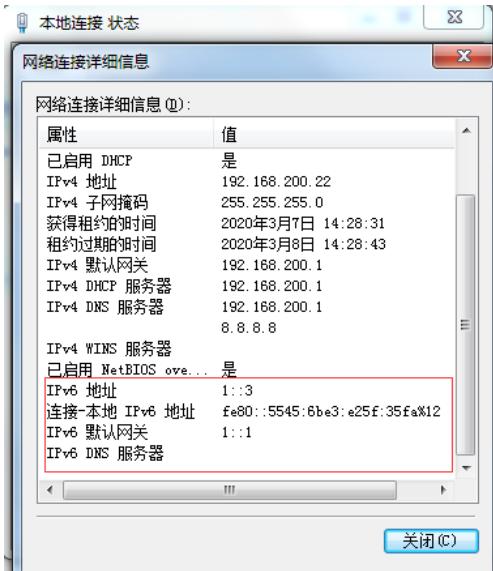
[FW2]security-zone name Trust
[FW2-security-zone-Trust]import interface GigabitEthernet 1/0/3
[FW2-security-zone-Trust]quit

FW2 IPV6 IPSEC+IKE预共享密钥关键配置点:
[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 keychain james
[FW2-ike-keychain-james]pre-shared-key address ipv6 3::1 64 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 ipv6 3::1 64
[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 james 1 isakmp
[FW2-ipsec-ipv6-policy-isakmp-james-1]security acl ipv6 3000
[FW2-ipsec-ipv6-policy-isakmp-james-1]transform-set james
[FW2-ipsec-ipv6-policy-isakmp-james-1]ike-profile james
[FW2-ipsec-ipv6-policy-isakmp-james-1]remote-address ipv6 3::1
[FW2-ipsec-ipv6-policy-isakmp-james-1]quit
[FW2]int gi 1/0/2
[FW2-GigabitEthernet1/0/2]ipsec apply ipv6-policy james
[FW2-GigabitEthernet1/0/2]quit

```

测试:

物理机填写IPV6地址:



物理机能PING通SW1:

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 © 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:
请求超时。
来自 2::2 的回复: 时[0]=3ns
来自 2::2 的回复: 时[0]=3ns
来自 2::2 的回复: 时[0]=2ns

2::2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 3, 丢失 = 1 (25% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms, 最长 = 3ms, 平均 = 2ms

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

```

SW1能PING通物理机:

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 © 2009 Microsoft Corporation。保留所有权利。
MSR36-20_2 SS820V2-54QS-GE_4 F1060_1 F1060_3
port link-mode bridge
combo enable fiber
#
interface GigabitEthernet1/0/3
port link-mode bridge
combo enable fiber
#
interface GigabitEthernet1/0/4
port link-mode bridge
combo enable fiber
<SW1> ping ipv6 1::3
Ping6(56 data bytes) 2::2 --> 1::3, press CTRL_C to break
56 bytes from 1::3, icmp_seq0 hlim=126 time=5.000 ms
56 bytes from 1::3, icmp_seq1 hlim=126 time=2.000 ms
56 bytes from 1::3, icmp_seq2 hlim=126 time=2.000 ms
56 bytes from 1::3, icmp_seq3 hlim=126 time=3.000 ms
56 bytes from 1::3, icmp_seq4 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 = 2.000/3.000/5.000/1.095 ms
<SW1>%Mar 8 09:05:16:308 2020 SW1 PING/6/PING_STATISTICS: Ping6 statistics for 1::3: 5 pa
cket(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/std-de
v = 2.000/3.000/5.000/1.095 ms.

```

查看FW1的IPSEC显示信息:

```

[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 01
[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 tunnel
Tunnel ID: 0
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
SA's SPI:
    outbound: 4250926382 (0xfd5ffd2e) [ESP]
    inbound: 875399137 (0x342d87e1) [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 875399137 4250926382 Active  
[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 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: 3::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: --  
[FW2]
```

```
[FW2]dis ipsec cu
[FW2]dis ipsec tunnel
Tunnel ID: 0
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
SA's SPI:
    outbound: 875399137 (0x342d87e1) [ESP]
    inbound: 4250926382 (0xfd5ffd2e) [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 4250926382 875399137 Active  
[FW2]
```

```
[FW2]dis ipsec tunnel brief
Tunn-id Src Address     Dst Address     Inbound SPI   Outbound SPI Status
0        4::1           3::1           4250926382   875399137   Active
[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+IKE预共享密钥已完成！