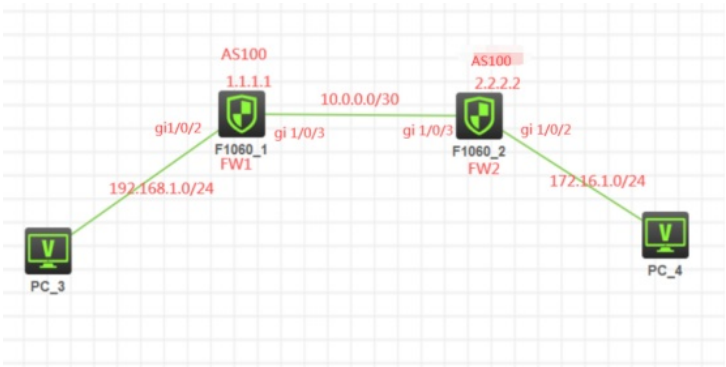
F1060 IBGP MD5认证典型组网配置案例

设备部署方式 H3C模拟器 韦家宁 2020-03-30 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IBGP MD5认证的典型组网。为了实现PC之间相互PING通，本案例采用IBGP的方式实现，同时为了保证IBGP邻居的合法性，因此采用IBGP MD5加密认证。

配置步骤

1、按照网络拓扑图正确配置IP地址

2、FW1、FW2建立IBGP邻居关系

3、FW1与FW2之间采用IBGP MD5认证。

4、在FW1与FW2建立IBGP邻居之前，需要先建立OSPF邻居关系，使其loopback地址可达，并为后续的IBGP邻居关系的建立奠定基础。

配置关键点

FW1:

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW1
[FW1]acl basic 2002
[FW1-acl-ipv4-basic-2002]rule 0 permit source any
[FW1-acl-ipv4-basic-2002]quit
[FW1]
[FW1]zone-pair security source trust destination untrust
[FW1-zone-pair-security-Trust-Untrust]packet-filter 2002
[FW1-zone-pair-security-Trust-Untrust]quit
[FW1]
[FW1]zone-pair security source untrust destination trust
[FW1-zone-pair-security-Untrust-Trust]packet-filter 2002
[FW1-zone-pair-security-Untrust-Trust]quit
[FW1]
[FW1]zone-pair security source trust destination local
[FW1-zone-pair-security-Trust-Local]packet-filter 2002
[FW1-zone-pair-security-Trust-Local]quit
[FW1]
[FW1]zone-pair security source local destination trust
[FW1-zone-pair-security-Local-Trust]packet-filter 2002
[FW1-zone-pair-security-Local-Trust]quit
[FW1]
[FW1]zone-pair security source untrust destination local
[FW1-zone-pair-security-Untrust-Local]packet-filter 2002
[FW1-zone-pair-security-Untrust-Local]quit
[FW1]
[FW1]zone-pair security source local destination untrust
[FW1-zone-pair-security-Local-Untrust]packet-filter 2002
[FW1-zone-pair-security-Local-Untrust]quit
[FW1]
```

```
[FW1]zone-pair security source trust destination trust
[FW1-zone-pair-security-Trust-Trust]packet-filter 2002
[FW1-zone-pair-security-Trust-Trust]quit
[FW1]
[FW1]zone-pair security source untrust destination untrust
[FW1-zone-pair-security-Untrust-Untrust]packet-filter 2002
[FW1-zone-pair-security-Untrust-Untrust]quit
[FW1]int loopback 0
[FW1-LoopBack0]ip address 1.1.1.1 32
[FW1-LoopBack0]quit
[FW1]int gi 1/0/2
[FW1-GigabitEthernet1/0/2]ip address 192.168.1.1 24
[FW1-GigabitEthernet1/0/2]quit
[FW1]int gi 1/0/3
[FW1-GigabitEthernet1/0/3]des <connect to FW2>
[FW1-GigabitEthernet1/0/3]ip address 10.0.0.1 30
[FW1-GigabitEthernet1/0/3]quit
[FW1]security-zone name Trust
[FW1-security-zone-Trust]import interface GigabitEthernet 1/0/2
[FW1-security-zone-Trust]quit
[FW1]security-zone name Untrust
[FW1-security-zone-Untrust]import interface GigabitEthernet 1/0/3
[FW1-security-zone-Untrust]import interface LoopBack 0
[FW1-security-zone-Untrust]quit
[FW1]ospf 1 router-id 1.1.1.1
[FW1-ospf-1]area 0.0.0.0
[FW1-ospf-1-area-0.0.0.0]network 10.0.0.1 0.0.0.0
[FW1-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0
[FW1-ospf-1-area-0.0.0.0]quit
[FW1-ospf-1]quit
[FW1]bgp 100
[FW1-bgp-default]router-id 1.1.1.1
[FW1-bgp-default]peer 2.2.2.2 as-number 100
[FW1-bgp-default]peer 2.2.2.2 password simple admin
[FW1-bgp-default]peer 2.2.2.2 connect-interface LoopBack 0
[FW1-bgp-default]address-family ipv4 unicast
[FW1-bgp-default-ipv4]peer 2.2.2.2 enable
[FW1-bgp-default-ipv4]network 192.168.1.0 255.255.255.0
[FW1-bgp-default-ipv4]quit
[FW1-bgp-default]quit
```

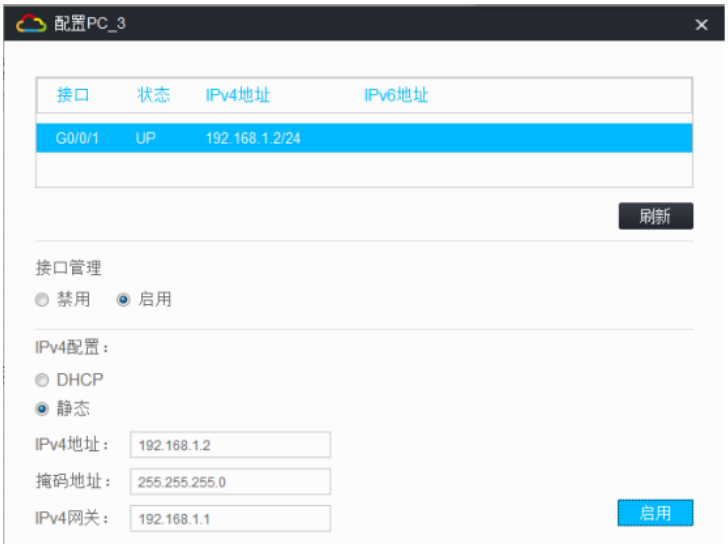
FW2：

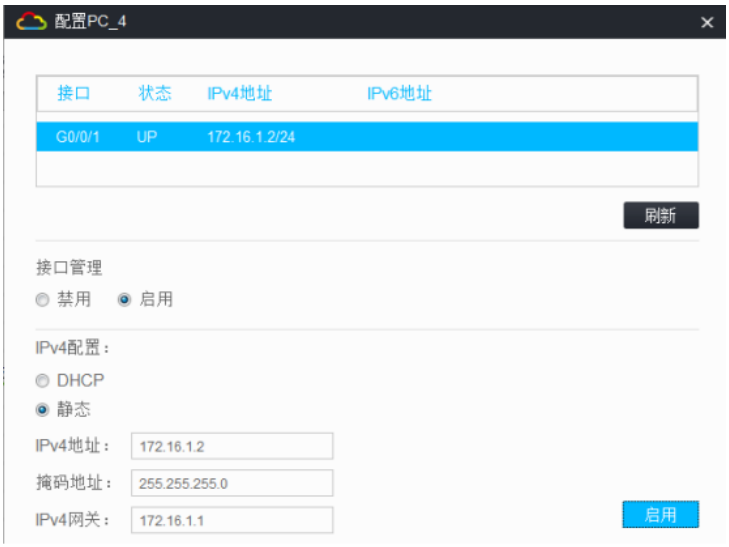
```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW2
[FW2]acl basic 2002
[FW2-acl-ipv4-basic-2002]rule 0 permit source any
[FW2-acl-ipv4-basic-2002]quit
[FW2]
[FW2]zone-pair security source trust destination untrust
[FW2-zone-pair-security-Trust-Untrust]packet-filter 2002
[FW2-zone-pair-security-Trust-Untrust]quit
[FW2]
[FW2]zone-pair security source untrust destination trust
[FW2-zone-pair-security-Untrust-Trust]packet-filter 2002
[FW2-zone-pair-security-Untrust-Trust]quit
[FW2]
[FW2]zone-pair security source trust destination local
[FW2-zone-pair-security-Trust-Local]packet-filter 2002
[FW2-zone-pair-security-Trust-Local]quit
[FW2]
[FW2]zone-pair security source local destination trust
[FW2-zone-pair-security-Local-Trust]packet-filter 2002
[FW2-zone-pair-security-Local-Trust]quit
```

```
[FW2]
[FW2]zone-pair security source untrust destination local
[FW2-zone-pair-security-Untrust-Local]packet-filter 2002
[FW2-zone-pair-security-Untrust-Local]quit
[FW2]
[FW2]zone-pair security source local destination untrust
[FW2-zone-pair-security-Local-Untrust]packet-filter 2002
[FW2-zone-pair-security-Local-Untrust]quit
[FW2]
[FW2]zone-pair security source trust destination trust
[FW2-zone-pair-security-Trust-Trust]packet-filter 2002
[FW2-zone-pair-security-Trust-Trust]quit
[FW2]
[FW2]zone-pair security source untrust destination untrust
[FW2-zone-pair-security-Untrust-Untrust]packet-filter 2002
[FW2-zone-pair-security-Untrust-Untrust]quit
[FW2]int loopback 0
[FW2-LoopBack0]ip address 2.2.2.2 32
[FW2-LoopBack0]quit
[FW2]int gi 1/0/2
[FW2-GigabitEthernet1/0/2]ip address 172.16.1.1 24
[FW2-GigabitEthernet1/0/2]quit
[FW2]int gi 1/0/3
[FW2-GigabitEthernet1/0/3]des <connect to FW1>
[FW2-GigabitEthernet1/0/3]ip address 10.0.0.2 30
[FW2-GigabitEthernet1/0/3]quit
[FW2]security-zone name Trust
[FW2-security-zone-Trust]import interface GigabitEthernet 1/0/2
[FW2-security-zone-Trust]quit
[FW2]security-zone name Untrust
[FW2-security-zone-Untrust]import interface LoopBack 0
[FW2-security-zone-Untrust]import interface GigabitEthernet 1/0/3
[FW2-security-zone-Untrust]quit
[FW2]ospf 1 router-id 2.2.2.2
[FW2-ospf-1]area 0.0.0.0
[FW2-ospf-1-area-0.0.0.0]network 10.0.0.2 0.0.0.0
[FW2-ospf-1-area-0.0.0.0]network 2.2.2.2 0.0.0.0
[FW2-ospf-1-area-0.0.0.0]quit
[FW2-ospf-1]quit
[FW2]bgp 100
[FW2-bgp-default]router-id 2.2.2.2
[FW2-bgp-default]peer 1.1.1.1 as-number 100
[FW2-bgp-default]peer 1.1.1.1 password simple admin
[FW2-bgp-default]peer 1.1.1.1 connect-interface LoopBack 0
[FW2-bgp-default]address-family ipv4 unicast
[FW2-bgp-default-ipv4]peer 1.1.1.1 enable
[FW2-bgp-default-ipv4]network 172.16.1.0 255.255.255.0
[FW2-bgp-default-ipv4]quit
[FW2-bgp-default]quit
```

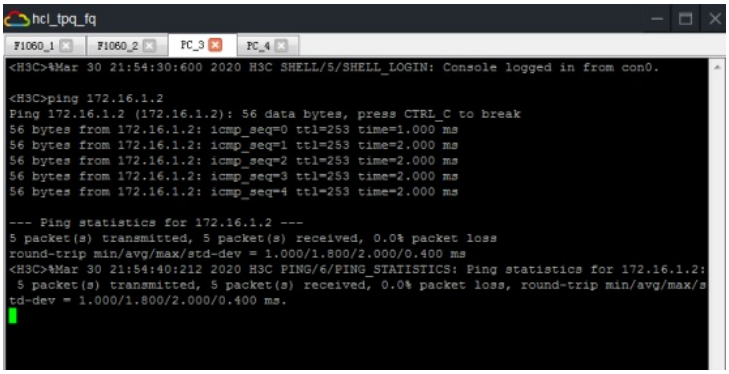
测试：

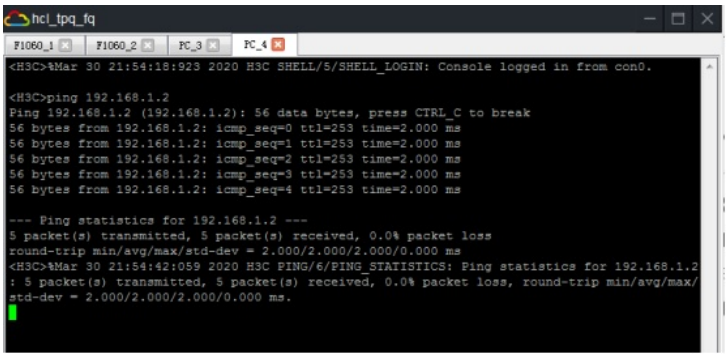
PC都填写IP地址：





PC之间可以相互PING通：





分别查看FW1、FW2的OSPF邻居信息：

```
[FW1]dis ospf peer

        OSPF Process 1 with Router ID 1.1.1.1
              Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 2.2.2.2         10.0.0.2        1   31         Full/BDR          GE1/0/3
[FW1]
```

```
[FW2]dis ospf peer

        OSPF Process 1 with Router ID 2.2.2.2
              Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 1.1.1.1         10.0.0.1        1   33         Full/DR           GE1/0/3
[FW2]
```

分别查看FW1、FW2的BGP邻居信息：

```
[FW1]dis bgp peer ipv4

 BGP local router ID: 1.1.1.1
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

  * - Dynamically created peer
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  2.2.2.2                 100        4        4    0       1 00:00:22 Established
[FW1]
```

```
[FW2]dis bgp peer ipv4

 BGP local router ID: 2.2.2.2
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

  * - Dynamically created peer
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  1.1.1.1                 100        4        4    0       1 00:00:37 Established
[FW2]
```

分别查看FW1、FW2的路由表：

```
[FW1]dis ip routing-table

Destinations : 19       Routes : 19

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
1.1.1.1/32         Direct  0   0           127.0.0.1       InLoop0
2.2.2.2/32         O_INTRA 10  1           10.0.0.2        GE1/0/3
10.0.0.0/30        Direct  0   0           10.0.0.1        GE1/0/3
10.0.0.0/32        Direct  0   0           10.0.0.1        GE1/0/3
10.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
10.0.0.3/32        Direct  0   0           10.0.0.1        GE1/0/3
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
172.16.1.0/24      BGP     255 0           2.2.2.2         GE1/0/3
192.168.1.0/24     Direct  0   0           192.168.1.1     GE1/0/2
192.168.1.0/32     Direct  0   0           192.168.1.1     GE1/0/2
192.168.1.1/32     Direct  0   0           127.0.0.1       InLoop0
192.168.1.255/32   Direct  0   0           192.168.1.1     GE1/0/2
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
[FW1]
```

```
[FW2]dis ip routing-table

Destinations : 19       Routes : 19

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
1.1.1.1/32         O_INTRA 10  1           10.0.0.1        GE1/0/3
2.2.2.2/32         Direct  0   0           127.0.0.1       InLoop0
10.0.0.0/30        Direct  0   0           10.0.0.2        GE1/0/3
10.0.0.0/32        Direct  0   0           10.0.0.2        GE1/0/3
10.0.0.2/32        Direct  0   0           127.0.0.1       InLoop0
10.0.0.3/32        Direct  0   0           10.0.0.2        GE1/0/3
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
172.16.1.0/24      Direct  0   0           172.16.1.1      GE1/0/2
172.16.1.0/32      Direct  0   0           172.16.1.1      GE1/0/2
172.16.1.1/32      Direct  0   0           127.0.0.1       InLoop0
172.16.1.255/32    Direct  0   0           172.16.1.1      GE1/0/2
192.168.1.0/24     BGP     255 0           1.1.1.1         GE1/0/3
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
[FW2]
```

至此，F1060 IBGP MD5认证典型组网配置anli已完成！