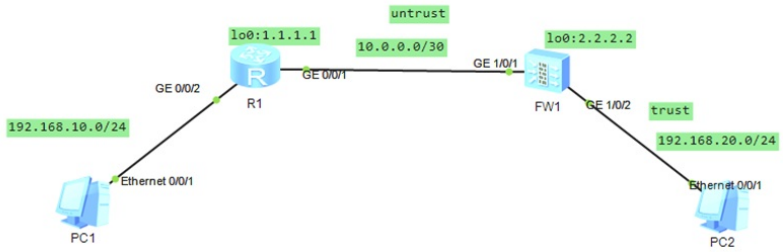
# 【MVS】华为防火墙路由模式典型组网配置案例-IBGP

网络相关 韦家宁 2024-09-13 发表

## 组网及说明




组网说明：

本案例采用ENSP模拟器的防火墙来部署路由模式的典型配置，安全域在网络拓扑图中已经有了明确的标识，全网先通过OSPF建立邻居关系，后续通过IBGP路由协议实现PC之间的互通。全网BGP AS号为100.

配置思路：

1、按照网络拓扑图配置IP地址和、OSPF、IBGP。

2、配置防火墙的安全域和安全策略。

## 配置步骤

R1：

```
<Huawei>u t m
Info: Current terminal monitor is off.
<Huawei>u t d
Info: Current terminal debugging is off.
<Huawei>system
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]int gi 0/0/2
[R1-GigabitEthernet0/0/2]ip address 192.168.10.1 24
[R1-GigabitEthernet0/0/2]quit
[R1]int gi 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.0.1 30
[R1-GigabitEthernet0/0/1]quit
[R1]int loopback 0
[R1-LoopBack0]ip address 1.1.1.1 32
[R1-LoopBack0]quit
[R1]ospf 1 router-id 1.1.1.1
[R1-ospf-1]area 0.0.0.0
[R1-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.3
[R1-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]quit
[R1-ospf-1]quit

[R1]bgp 100
[R1-bgp]router-id 1.1.1.1
[R1-bgp]peer 2.2.2.2 as-number 100
[R1-bgp]peer 2.2.2.2 connect-interface LoopBack 0
[R1-bgp]ipv4-family unicast
[R1-bgp-af-ipv4]peer 2.2.2.2 enable
[R1-bgp-af-ipv4]network 192.168.10.0 24
[R1-bgp-af-ipv4]quit
[R1-bgp]quit
```

FW1：

```
<USG6000V1>u t m
Info: Current terminal monitor is off.
<USG6000V1>u t d
Info: Current terminal debugging is off.
<USG6000V1>system
Enter system view, return user view with Ctrl+Z.
[USG6000V1]sysname FW1
[FW1]int gi 1/0/1
[FW1-GigabitEthernet1/0/1]ip address 10.0.0.2 30
[FW1-GigabitEthernet1/0/1]quit
[FW1]int gi 1/0/2
[FW1-GigabitEthernet1/0/2]ip address 192.168.20.1 24
[FW1-GigabitEthernet1/0/2]quit
[FW1]int loopback 0
[FW1-LoopBack0]ip address 2.2.2.2 32
[FW1-LoopBack0]quit
[FW1]ospf 1 router-id 2.2.2.2
[FW1-ospf-1]area 0.0.0.0
[FW1-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.3
[FW1-ospf-1-area-0.0.0.0]network 2.2.2.2 0.0.0.0
[FW1-ospf-1-area-0.0.0.0]quit
[FW1-ospf-1]quit

[FW1]bgp 100
[FW1-bgp]router-id 2.2.2.2
[FW1-bgp]peer 1.1.1.1 as-number 100
[FW1-bgp]peer 1.1.1.1 connect-interface LoopBack 0
[FW1-bgp]ipv4-family unicast
[FW1-bgp-af-ipv4]peer 1.1.1.1 enable
[FW1-bgp-af-ipv4]network 192.168.20.0 24
[FW1-bgp-af-ipv4]quit
[FW1-bgp]quit


[FW1]firewall zone trust
[FW1-zone-trust]add int gi 1/0/2
[FW1-zone-trust]quit
[FW1]firewall zone untrust
[FW1-zone-untrust]add int gi 1/0/1
[FW1-zone-untrust]quit
[FW1]security-policy
[FW1-policy-security]default action permit
Warning:Setting the default packet filtering to permit poses security risks. You
 are advised to configure the security policy based on the actual data flows. Ar
e you sure you want to continue?[Y/N]y
[FW1-policy-security]quit
```

分别查看FW1和R1的OSPF邻居关系建立的情况，已完成建立！

```
[FW1]dis ospf peer
2024-09-13 04:23:20.780

       OSPF Process 1 with Router ID 2.2.2.2
             Neighbors

 Area 0.0.0.0 interface 10.0.0.2(GigabitEthernet1/0/1)'s neighbors
 Router ID: 1.1.1.1          Address: 10.0.0.1
   State: Full  Mode:Nbr is  Slave  Priority: 1
   DR: 10.0.0.1  BDR: 10.0.0.2  MTU: 0
   Dead timer due in 35  sec
   Retrans timer interval: 5
   Neighbor is up for 00:02:52
   Authentication Sequence: [ 0 ]
```

```
[R1]dis ospf peer

       OSPF Process 1 with Router ID 1.1.1.1
             Neighbors

 Area 0.0.0.0 interface 10.0.0.1(GigabitEthernet0/0/1)'s neighbors
 Router ID: 2.2.2.2          Address: 10.0.0.2
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 10.0.0.1  BDR: 10.0.0.2  MTU: 0
   Dead timer due in 36  sec
   Retrans timer interval: 5
   Neighbor is up for 00:03:02
   Authentication Sequence: [ 0 ]
```

分别查看FW1和R1的BGP邻居关系建立的情况，已完成建立！

```
[R1]dis bgp peer

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

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State Pre
fRcv

  2.2.2.2         4         100        3        4     0 00:00:15 Established
    1
```

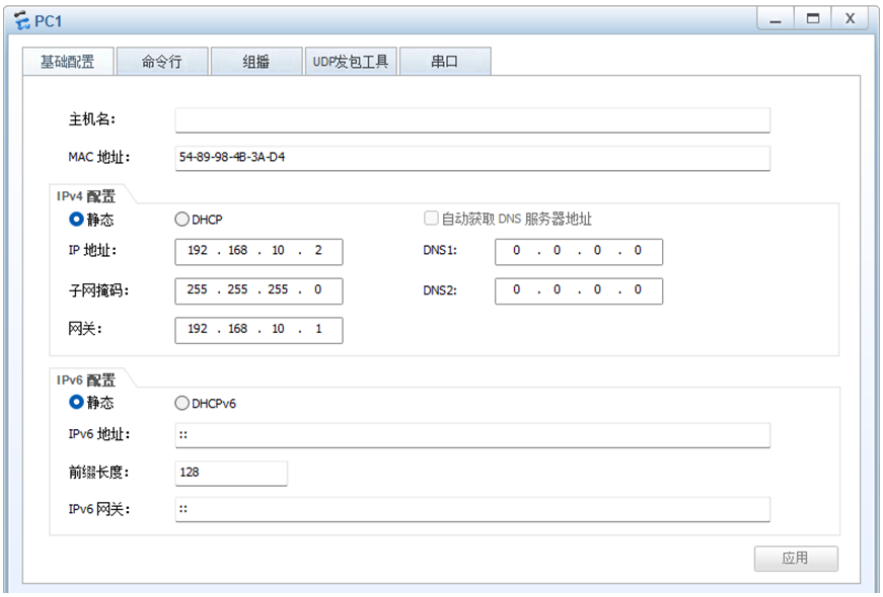
```
[FW1]dis bgp peer
2024-09-13 04:22:22.580

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

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State Pre
fRcv

  1.1.1.1         4         100        3        3     0 00:00:47 Established
    1
```

使用dis ip routing-table命令查看FW1和R1的路由表，均能学习到对端传递过来的路由。

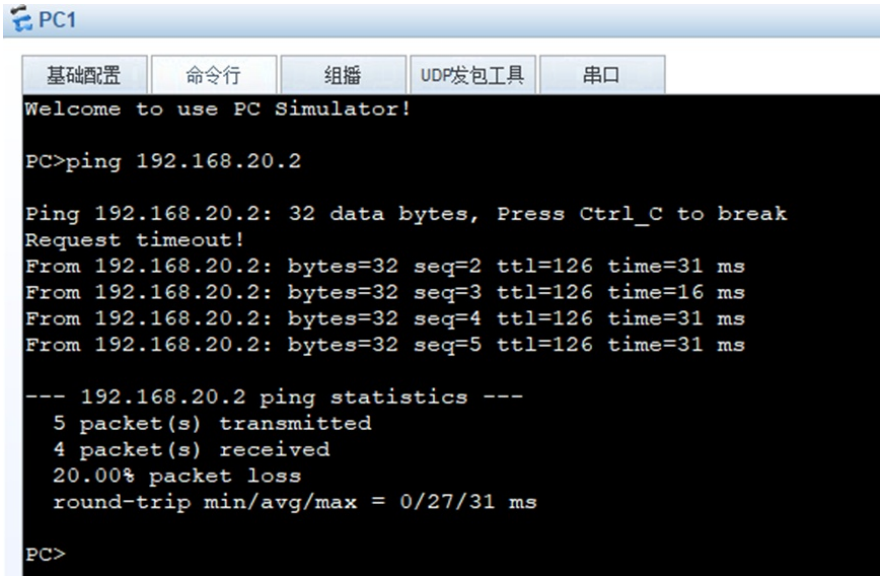
```
[FW1]dis ip routing-table
2024-09-13 04:22:33.400
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  OSPF    10   1           D   10.0.0.1        GigabitEthernet
1/0/1
        2.2.2.2/32  Direct  0    0           D   127.0.0.1       LoopBack0
       10.0.0.0/30  Direct  0    0           D   10.0.0.2        GigabitEthernet
1/0/1
       10.0.0.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
1/0/1
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   192.168.10.0/24  IBGP    255  0          RD   1.1.1.1         GigabitEthernet
1/0/1
   192.168.20.0/24  Direct  0    0           D   192.168.20.1    GigabitEthernet
1/0/2
   192.168.20.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
1/0/2
```

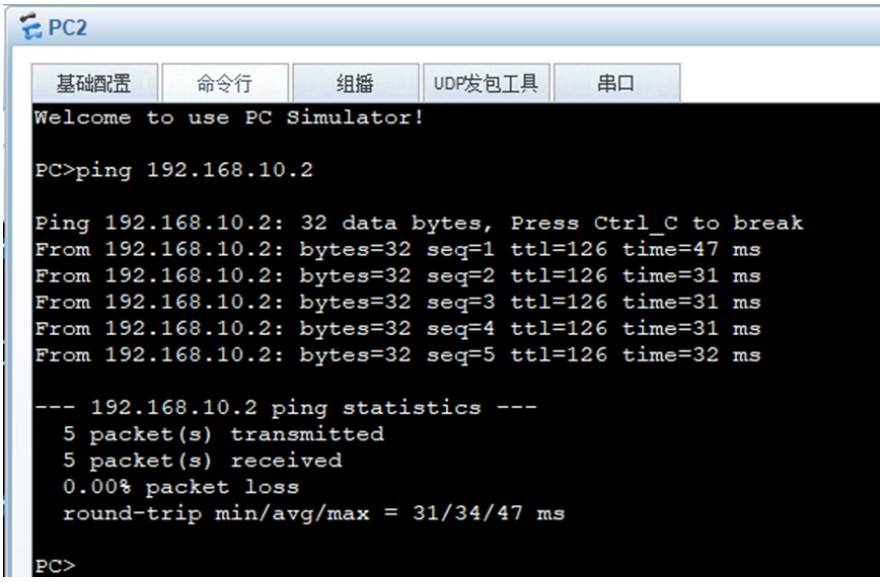
```
[R1]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
        2.2.2.2/32  OSPF    10   1           D   10.0.0.2        GigabitEthernet
0/0/1
       10.0.0.0/30  Direct  0    0           D   10.0.0.1        GigabitEthernet
0/0/1
       10.0.0.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   192.168.10.0/24  Direct  0    0           D   192.168.10.1    GigabitEthernet
0/0/2
   192.168.10.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/2
   192.168.20.0/24  IBGP    255  0          RD   2.2.2.2         GigabitEthernet
0/0/1
```

PC分别填写IP地址，且能相互PING通。


PC1
基础配置
命令行
组播
UDP发包工具
串口
主机名:
MAC 地址:
54-89-98-4B-3A-D4
IPv4 配置
静态
DHCP
自动获取 DNS 服务器地址
IP 地址:
192 . 168 . 10 . 2
DNS1:
0 . 0 . 0 . 0
子网掩码:
255 . 255 . 255 . 0
DNS2:
0 . 0 . 0 . 0
网关:
192 . 168 . 10 . 1
IPv6 配置
静态
DHCPv6
IPv6 地址:
::
前缀长度:
128
IPv6 网关:
::
应用


PC2
基础配置
命令行
组播
UDP发包工具
串口
主机名:
MAC 地址:
54-89-98-CF-73-AE
IPv4 配置
静态
DHCP
自动获取 DNS 服务器地址
IP 地址:
192 . 168 . 20 . 2
DNS1:
0 . 0 . 0 . 0
子网掩码:
255 . 255 . 255 . 0
DNS2:
0 . 0 . 0 . 0
网关:
192 . 168 . 20 . 1
IPv6 配置
静态
DHCPv6
IPv6 地址:
::
前缀长度:
128
IPv6 网关:
::
应用


PC1
基础配置
命令行
组播
UDP发包工具
串口
Welcome to use PC Simulator!
PC>ping 192.168.20.2
Ping 192.168.20.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 192.168.20.2: bytes=32 seq=2 ttl=126 time=31 ms
From 192.168.20.2: bytes=32 seq=3 ttl=126 time=16 ms
From 192.168.20.2: bytes=32 seq=4 ttl=126 time=31 ms
From 192.168.20.2: bytes=32 seq=5 ttl=126 time=31 ms
--- 192.168.20.2 ping statistics ---
5 packet(s) transmitted
4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 0/27/31 ms
PC>




至此，华为防火墙路由模式典型组网配置案例（IBGP）已完成!