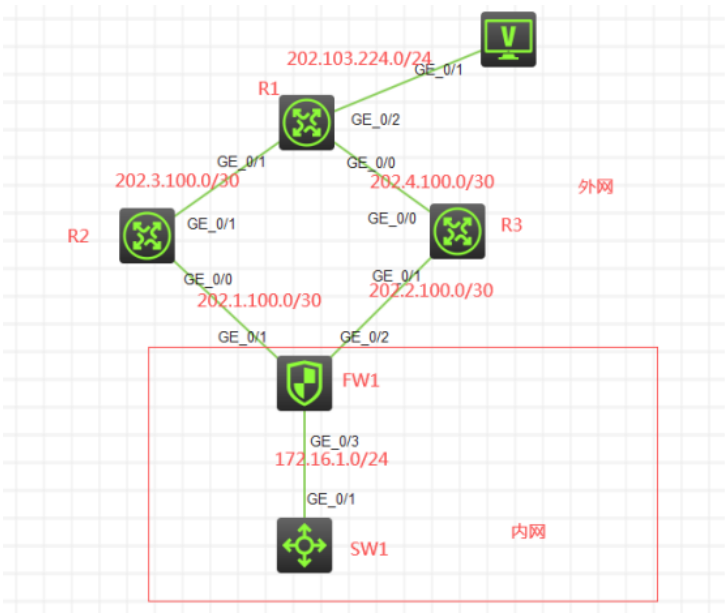
F1060 单设备双NAT冗余典型组网配置1（路由备份的方式）

ACL　设备部署方式　**韦家宁**　2021-01-23 发表

组网及说明



组网说明：

本案例采用H3C HCL模拟器的F1060防火墙来模拟器双NAT出口。在网络拓扑中已经明确标识了内网和外网，FW1作为内网的出口设备，承担地址转换的任务。由于防火墙有双出口，为了演示达到双出口冗余的需求，通过路由备份的方式实现内网的IP优先走R2方向去往外网服务器，当R2链路故障时，能走R3去往服务器。外网走静态路由协议，FW1配置默认路由指向到外网。

配置步骤

FW1 :

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW1
[FW1]acl basic 2000
[FW1-acl-ipv4-basic-2000]rule 0 permit source any
[FW1-acl-ipv4-basic-2000]quit
[FW1]zone-pair security source trust destination untrust
[FW1-zone-pair-security-Trust-Untrust]packet-filter 2000
[FW1-zone-pair-security-Trust-Untrust]quit
[FW1]zone-pair security source untrust destination trust
[FW1-zone-pair-security-Untrust-Trust]packet-filter 2000
[FW1-zone-pair-security-Untrust-Trust]quit
[FW1]zone-pair security source trust destination local
[FW1-zone-pair-security-Trust-Local]packet-filter 2000
[FW1-zone-pair-security-Trust-Local]quit
[FW1]zone-pair security source local destination trust
[FW1-zone-pair-security-Local-Trust]packet-filter 2000
[FW1-zone-pair-security-Local-Trust]quit
[FW1]zone-pair security source untrust destination local
[FW1-zone-pair-security-Untrust-Local]packet-filter 2000
[FW1-zone-pair-security-Untrust-Local]quit
[FW1]zone-pair security source local destination untrust
[FW1-zone-pair-security-Local-Untrust]packet-filter 2000
[FW1-zone-pair-security-Local-Untrust]quit
[FW1]zone-pair security source trust destination trust
[FW1-zone-pair-security-Trust-Trust]packet-filter 2000
[FW1-zone-pair-security-Trust-Trust]quit
[FW1]zone-pair security source untrust destination untrust
[FW1-zone-pair-security-Untrust-Untrust]packet-filter 2000
[FW1-zone-pair-security-Untrust-Untrust]quit
[FW1]vlan 10
[FW1-vlan10]quit
[FW1]int vlan 10
[FW1-Vlan-interface10]ip address 172.16.1.254 24
[FW1-Vlan-interface10]quit
[FW1]int gi 1/0/3
[FW1-GigabitEthernet1/0/3]ip address 172.16.1.254 24
[FW1-GigabitEthernet1/0/3]quit
[FW1]acl basic 2001
[FW1-acl-ipv4-basic-2001]des to_R2
[FW1-acl-ipv4-basic-2001]rule 0 permit source any
[FW1-acl-ipv4-basic-2001]quit
[FW1]acl basic 2002
[FW1-acl-ipv4-basic-2002]des to_R3
[FW1-acl-ipv4-basic-2002]rule 0 permit source any
[FW1-acl-ipv4-basic-2002]quit
[FW1]nat address-group 1
[FW1-address-group-1]address 202.2.100.3 202.2.100.4
[FW1-address-group-1]quit
[FW1]nat address-group 2
[FW1-address-group-2]address 202.1.100.3 202.1.100.4
[FW1-address-group-2]quit

[FW1]int gi 1/0/1
[FW1-GigabitEthernet1/0/1]ip address 202.1.100.2 28
[FW1-GigabitEthernet1/0/1]des <connect to R2>
[FW1-GigabitEthernet1/0/1]nat outbound 2001 address-group 2
[FW1-GigabitEthernet1/0/1]quit
```

[FW1]int gi 1/0/2

[FW1-GigabitEthernet1/0/2]ip address 202.2.100.2 28

[FW1-GigabitEthernet1/0/2]des <connect to R3>

配置关键点

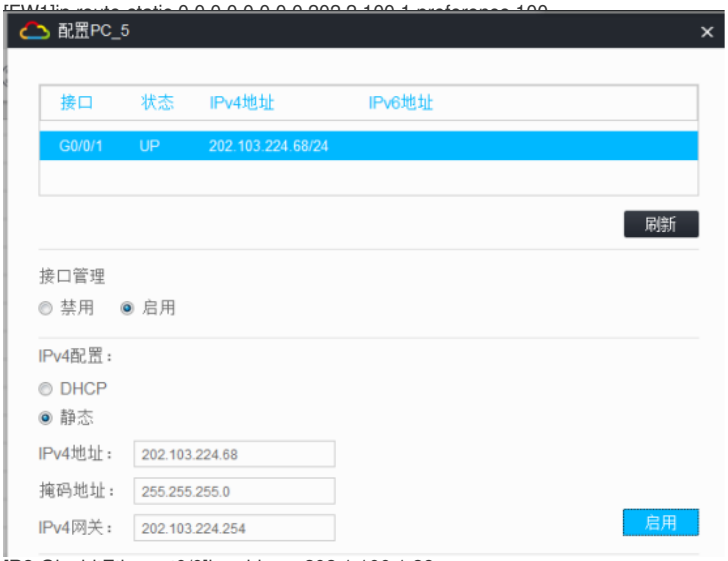
[FW1-GigabitEthernet1/0/2]nat outbound 2002 address-group 1

测试：

[FW1-GigabitEthernet1/0/2]quit

服务器填写IP地址：

[FW1]ip route-static 0.0.0.0 0.0.0.0 202.1.100.1



[R2-GigabitEthernet0/0]ip address 202.1.100.1 28

[R2-GigabitEthernet0/0]quit

SW1配置IP地址为172.16.1.1及网关：

[R2]int gi 0/1

<H3C>sys

[R2-GigabitEthernet0/1]des <connect to R1>

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

[R2-GigabitEthernet0/1]ip address 202.3.100.2 30

[H3C]sysname SW1

[R2-GigabitEthernet0/1]quit

[SW1]int gi 1/0/1

[R2]ip route-static 202.1.100.0 255.255.255.240 202.1.100.2

[SW1-GigabitEthernet1/0/1]port link-mode route

[R2]ip route-static 0.0.0.0 0.0.0.0 202.3.100.1

[SW1-GigabitEthernet1/0/1]ip address 172.16.1.1 24

[R2]ip ttl-expires enable

[SW1-GigabitEthernet1/0/1]quit

[R2]ip unreachables enable

[SW1]ip route-static 0.0.0.0 0.0.0.0 172.16.1.254

[SW1]ip ttl-expires enable

[SW1]ip unreachables enable

R3：

<H3C>sys

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

当双链路都正常时，采用tracert的方式确认172.16.1.1走的是R2方向去往服务器。

[H3C]sysname R3

```
<SW1>tracert 202.103.224.68
traceroute to 202.103.224.68 (202.103.224.68), 30 hops at most, 40 bytes each
s CTRL_C to break
 1  172.16.1.254 (172.16.1.254)  1.000 ms  2.000 ms  1.000 ms
 2  202.1.100.1 (202.1.100.1)  1.000 ms  1.000 ms  2.000 ms
 3  202.3.100.1 (202.3.100.1)  1.000 ms  1.000 ms  2.000 ms
 4  * * *
 5  *
<SW1>ping 202.103.224.68
Ping 202.103.224.68 (202.103.224.68): 56 data bytes, press CTRL_C to break
56 bytes from 202.103.224.68: icmp_seq=0 ttl=252 time=4.000 ms
56 bytes from 202.103.224.68: icmp_seq=1 ttl=252 time=2.000 ms
56 bytes from 202.103.224.68: icmp_seq=2 ttl=252 time=3.000 ms
56 bytes from 202.103.224.68: icmp_seq=3 ttl=252 time=3.000 ms
56 bytes from 202.103.224.68: icmp_seq=4 ttl=252 time=3.000 ms

--- Ping statistics for 202.103.224.68 ---
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>%Jan 23 11:16:35:714 2021 SW1 PING/6/PING_STATISTICS: Ping statistics fo
.68: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-t
ax/std-dev = 2.000/3.000/4.000/0.632 ms.
```

[R3]

<H3C>sys

当关闭去往R2的链路时，能去R3去往服务器，且网络不中断：

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

```
[FW1]int gi 1/0/1
[FW1-GigabitEthernet1/0/1]shu
[FW1-GigabitEthernet1/0/1]shutdown
%Jan 23 11:17:03:767 2021 FW1 IFNET/3/PHY_UPDOWN: -Context=1; Physic
ace GigabitEthernet1/0/1 changed to down.
%Jan 23 11:17:03:767 2021 FW1 IFNET/5/LINK_UPDOWN: -Context=1; Line
interface GigabitEthernet1/0/1 changed to down.
[FW1-GigabitEthernet1/0/1]
```

[R1-GigabitEthernet0/0]ip address 202.4.100.1 30

[R1-GigabitEthernet0/0]quit

[R1]int gi 0/1

[R1-GigabitEthernet0/1]des <connect to R2>

```
Ping 202.103.224.68 (202.103.224.68): 56 data bytes, press CTRL_C to break
56 bytes from 202.103.224.68: icmp_seq=0 ttl=252 time=5.000 ms
56 bytes from 202.103.224.68: icmp_seq=1 ttl=252 time=3.000 ms
56 bytes from 202.103.224.68: icmp_seq=2 ttl=252 time=4.000 ms
56 bytes from 202.103.224.68: icmp_seq=3 ttl=252 time=2.000 ms
56 bytes from 202.103.224.68: icmp_seq=4 ttl=252 time=2.000 ms

--- Ping statistics for 202.103.224.68 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.000/3.200/5.000/1.166 ms
<SW1>%Jan 23 11:20:17:467 2021 SW1 PING/6/PING_STATISTICS: Ping statistics for 202.1
.68: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min
ax/std-dev = 2.000/3.200/5.000/1.166 ms.

<SW1>tracert 202.103.224.68
traceroute to 202.103.224.68 (202.103.224.68), 30 hops at most, 40 bytes each packet
% CTRL_C to break
 1  172.16.1.254 (172.16.1.254)  1.000 ms  0.000 ms  1.000 ms
 2  202.2.100.1 (202.2.100.1)  2.000 ms  1.000 ms  1.000 ms
 3  202.4.100.1 (202.4.100.1)  2.000 ms  2.000 ms  2.000 ms
 4
```

至此，F1060防火墙单设备双NAT冗余备份典型组网配置实验已完成！