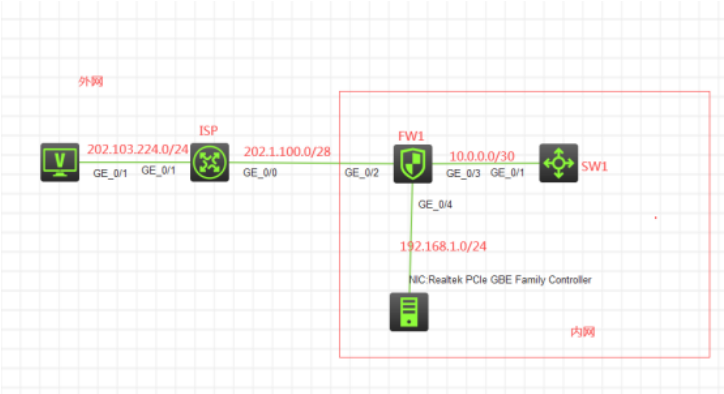
# F1060 双向NAT典型组网配置案例2（无固定公网地址映射）

NAT H3C模拟器 韦家宁 2020-03-07 发表

## 组网及说明




组网说明：

本案例采用H3C HCL模拟器来模拟实现双向NAT的组网，由于模拟器和本物理机的局限性，因此采用模拟器的S5820交换机开启WEB功能模拟成为WEB服务器。在该网络拓扑图中，内网和外网已经有了明确的标识，某局点申请了202.1.100.1这个公网IP地址，其中202.1.100.2用于与外网互联，同时也用于给内网WEB服务器的转换并对外网提供WEB服务，同时内网机子能通过使用外网IP地址来访问WEB服务器，因此在不使用NAT回流的前提下，采用双向NAT来实现此需求。

## 配置步骤

1、按照网络拓扑图正确配置IP地址

2、SW1开启WEB功能，并创建相应账户及赋予权限

3、SW1配置默认路由指向FW1

4、FW1配置默认路由指向外网，并配置静态路由指向SW1

5、FW1配置NAT，允许内网主机访问外网

6、FW1配置双向NAT，实现内网主机通过使用外网地址来访问WEB服务

## 配置关键点

ISP：

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname ISP
[ISP]int gi 0/1
[ISP-GigabitEthernet0/1]ip address 202.103.224.254 24
[ISP-GigabitEthernet0/1]quit
[ISP]int gi 0/0
[ISP-GigabitEthernet0/0]des <connect to FW1>
[ISP-GigabitEthernet0/0]ip address 202.1.100.1 28
[ISP-GigabitEthernet0/0]quit
```

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 FW1>
[SW1-GigabitEthernet1/0/1]ip address 10.0.0.2 30
[SW1-GigabitEthernet1/0/1]quit
[SW1]ip route-static 0.0.0.0 0.0.0.0 10.0.0.1
[SW1]ip http enable
[SW1]ip https enable
[SW1]local-user admin
New local user added.
```

```
[SW1-luser-manage-admin]password simple admin
[SW1-luser-manage-admin]service-type http https
[SW1-luser-manage-admin]authorization-attribute user-role network-admin
[SW1-luser-manage-admin]quit
```

FW1：

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW1
[FW1]acl basic 2001
[FW1-acl-ipv4-basic-2001]rule 0 permit source any
[FW1-acl-ipv4-basic-2001]quit
[FW1]
[FW1]zone-pair security source trust destination untrust
[FW1-zone-pair-security-Trust-Untrust]packet-filter 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 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 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 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 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 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 2001
[FW1-zone-pair-security-Trust-Trust]quit
[FW1]int gi 1/0/4
[FW1-GigabitEthernet1/0/4]ip address 192.168.1.1 24
[FW1-GigabitEthernet1/0/4]quit
[FW1]int gi 1/0/3
[FW1-GigabitEthernet1/0/3]des <connect to SW1>
[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 1/0/3
[FW1-security-zone-Trust]import interface GigabitEthernet 1/0/4
[FW1-security-zone-Trust]quit
```

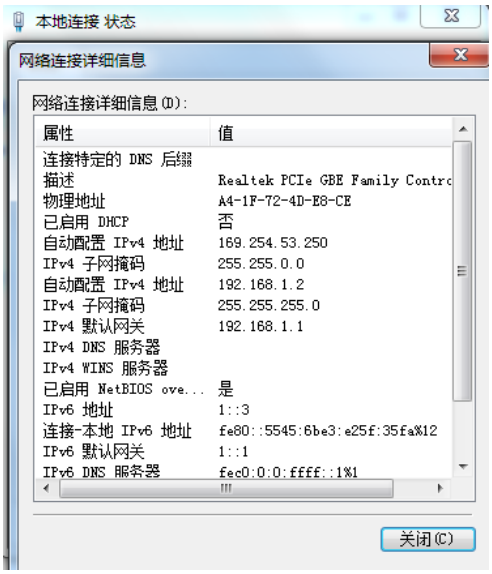
FW1 双向NAT关键配置点：

```
[FW1]acl basic 2000
[FW1-acl-ipv4-basic-2000]rule 0 permit source any
[FW1-acl-ipv4-basic-2000]quit
[FW1]int gi 1/0/2
[FW1-GigabitEthernet1/0/2]des <connect to ISP>
[FW1-GigabitEthernet1/0/2]ip address 202.1.100.2 28
[FW1-GigabitEthernet1/0/2]nat outbound 2000
[FW1-GigabitEthernet1/0/2]nat server protocol tcp global current-interface 80 inside 10.0.0.2 80
[FW1-GigabitEthernet1/0/2]nat server protocol tcp global current-interface 443 inside 10.0.0.2 443
[FW1-GigabitEthernet1/0/2]quit
[FW1]ip route-static 0.0.0.0 0.0.0.0 202.1.100.1
```

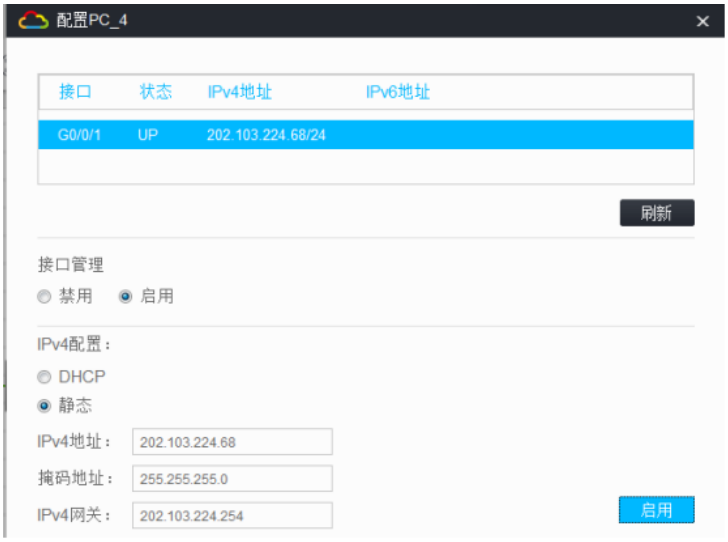
```
[FW1]acl basic 2002
[FW1-acl-ipv4-basic-2002]rule 0 permit source 192.168.1.0 0.0.0.255
[FW1-acl-ipv4-basic-2002]quit
[FW1]int gi 1/0/3
[FW1-GigabitEthernet1/0/3]nat outbound 2002
[FW1-GigabitEthernet1/0/3]nat server protocol tcp global 202.1.100.2 80 inside 10.0.0.2 80
[FW1-GigabitEthernet1/0/3]nat server protocol tcp global 202.1.100.2 443 inside 10.0.0.2 443
[FW1-GigabitEthernet1/0/3]quit
[FW1]security-zone name Untrust
[FW1-security-zone-Untrust]import interface GigabitEthernet 1/0/2
[FW1-security-zone-Untrust]quit
[FW1]int gi 1/0/4
[FW1-GigabitEthernet1/0/4]nat outbound 2002
[FW1-GigabitEthernet1/0/4]nat server protocol tcp global 202.1.100.2 80 inside 10.0.0.2 80
[FW1-GigabitEthernet1/0/4]nat server protocol tcp global 202.1.100.2 443 inside 10.0.0.2 443
[FW1-GigabitEthernet1/0/4]quit
```

测试：

内网机填写IP地址：

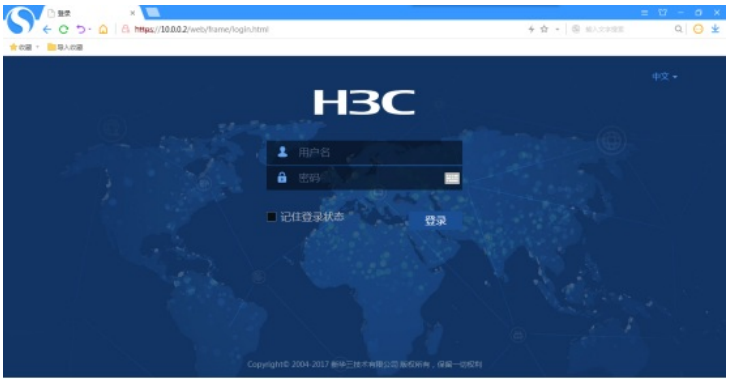



外网PC填写IP地址：




内网PC能PING通外网PC：


内网PC能使用内网地址10.0.0.2访问WEB服务器SW1：




内网PC使用202.1.100.2这个外网地址也可访问内网WEB服务器SW1：


[FW1]dis nat server
NAT internal server information:
  Totally 6 internal servers.
  Interface: GigabitEthernet1/0/2
    Protocol: 6(TCP)
    Global IP/port: 202.1.100.2/80
    Local IP/port : 10.0.0.2/80
    NAT counting  : 0
    Config status : Active

  Interface: GigabitEthernet1/0/2
    Protocol: 6(TCP)
    Global IP/port: 202.1.100.2/443
    Local IP/port : 10.0.0.2/443
    NAT counting  : 0
    Config status : Active

  Interface: GigabitEthernet1/0/3
    Protocol: 6(TCP)
    Global IP/port: 202.1.100.2/80
    Local IP/port : 10.0.0.2/80
    NAT counting  : 0
    Config status : Active

Interface: GigabitEthernet1/0/3
Protocol: 6(TCP)
Global IP/port: 202.1.100.2/443
Local IP/port : 10.0.0.2/443
NAT counting : 0
Config status : Active

Interface: GigabitEthernet1/0/4
Protocol: 6(TCP)
Global IP/port: 202.1.100.2/80
Local IP/port : 10.0.0.2/80
NAT counting : 0
Config status : Active

Interface: GigabitEthernet1/0/4
Protocol: 6(TCP)
Global IP/port: 202.1.100.2/443
Local IP/port : 10.0.0.2/443
NAT counting : 0
Config status : Active

[FW1]

```
[FW1]dis nat outbound
NAT outbound information:
  Totally 3 NAT outbound rules.
  Interface: GigabitEthernet1/0/2
    ACL: 2000
    Address group ID: ---
    Port-preserved: N        NO-PAT: N  Reversible: N
    NAT counting: 0
    Config status: Active

  Interface: GigabitEthernet1/0/3
    ACL: 2002
    Address group ID: ---
    Port-preserved: N        NO-PAT: N  Reversible: N
    NAT counting: 0
    Config status: Active

  Interface: GigabitEthernet1/0/4
    ACL: 2002
    Address group ID: ---
    Port-preserved: N        NO-PAT: N  Reversible: N
    NAT counting: 0
    Config status: Active

[FW1]
```

至此，F1060双向NAT典型组网配置案例2（无固公网地址映射）已完成！