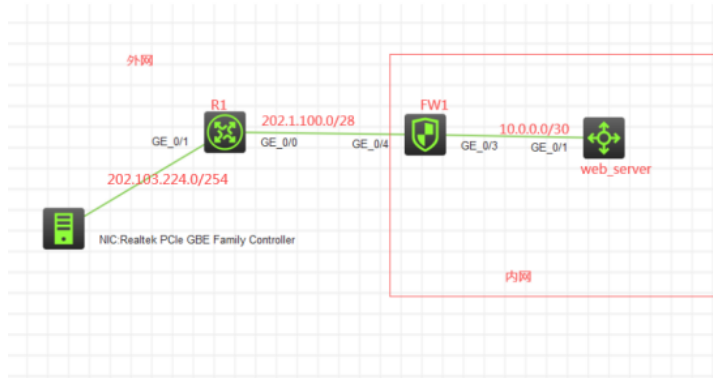


知 F1060 NAT server典型组网配置案例1 (有固定公网地址转换)

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模拟器的F1060来模拟NAT server典型组网配置，内网和外网在网络拓扑图中已经有了明确的标识，FW1作为内网的出口设备，不仅保护内网的安全，也提供地址转换的服务。内网申请了202.1.100.2-202.1.100.3这两个公网地址，其中202.1.100.2用于FW1与外网互联使用。202.1.100.3用于给内网的WEB服务器转换并对外网提供WEB服务。由于模拟器及物理机的局限性，因此采用H3C HCL模拟器的S5820交换机开启WEB功能模拟成WEB服务器。

配置步骤

- 1、按照网络拓扑图正确配置IP地址
- 2、Web_server开启WEB功能，并创建相应账户及赋予权限
- 3、FW1配置NAT地址转换，并配置默认路由指向外网
- 4、FW1配置nat server，并发布内网的WEB服务器

配置关键点

Web_server:

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname web_server
[web_server]int gi 1/0/1
[web_server-GigabitEthernet1/0/1]port link-mode route
[web_server-GigabitEthernet1/0/1]des <connect to FW1>
[web_server-GigabitEthernet1/0/1]ip address 10.0.0.2 30
[web_server-GigabitEthernet1/0/1]quit
[web_server]ip route-static 0.0.0.0 0.0.0.0 10.0.0.1
[web_server]ip http enable
[web_server]ip https enable
[web_server]local-user admin
New local user added.
[web_server-luser-manage-admin]password simple admin
[web_server-luser-manage-admin]service-type http https
[web_server-luser-manage-admin]authorization-attribute user-role network-admin
[web_server-luser-manage-admin]quit
[web_server]
```

ISP:

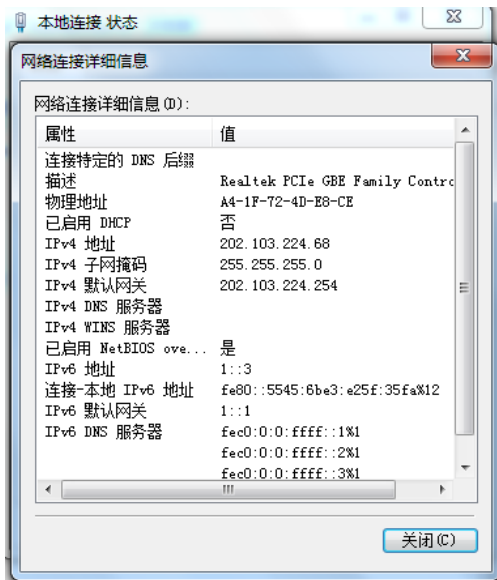
```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname ISP
[ISP]int gi 0/1
[ISP-GigabitEthernet0/1]ip address 202.103.224.254 24
[ISP-GigabitEthernet0/1]quit
[ISP]int gi 0/0
[ISP-GigabitEthernet0/0]des <connect to FW1>
[ISP-GigabitEthernet0/0]ip address 202.1.100.1 28
[ISP-GigabitEthernet0/0]quit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

```
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]int gi 1/0/3
[FW1-GigabitEthernet1/0/3]des <connect to web_server>
[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]quit
```

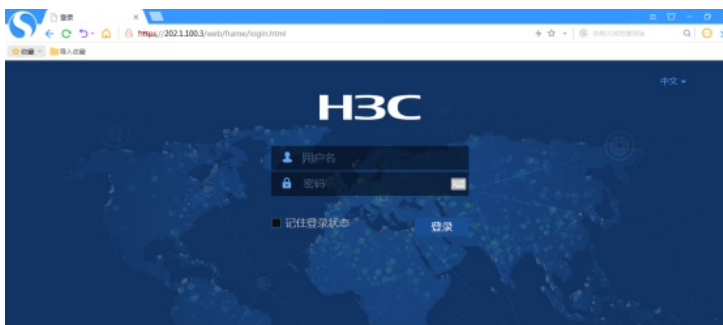
FW1 NAT及NAT server关键配置点:

```
[FW1]acl basic 2000
[FW1-acl-ipv4-basic-2000]rule 0 permit source any
[FW1-acl-ipv4-basic-2000]quit
[FW1]int gi 1/0/4
[FW1-GigabitEthernet1/0/4]des <connect to ISP>
[FW1-GigabitEthernet1/0/4]ip address 202.1.100.2 28
[FW1-GigabitEthernet1/0/4]nat outbound 2000
[FW1-GigabitEthernet1/0/4]nat server protocol tcp global 202.1.100.3 80 inside 10.0.0.2 80
[FW1-GigabitEthernet1/0/4]nat server protocol tcp global 202.1.100.3 443 inside 10.0.0.2 443
[FW1-GigabitEthernet1/0/4]quit
[FW1]ip route-static 0.0.0.0 0.0.0.0 202.1.100.1
[FW1]security-zone name Untrust
[FW1-security-zone-Untrust]import interface GigabitEthernet 1/0/4
[FW1-security-zone-Untrust]quit
```

物理机填写IP地址:



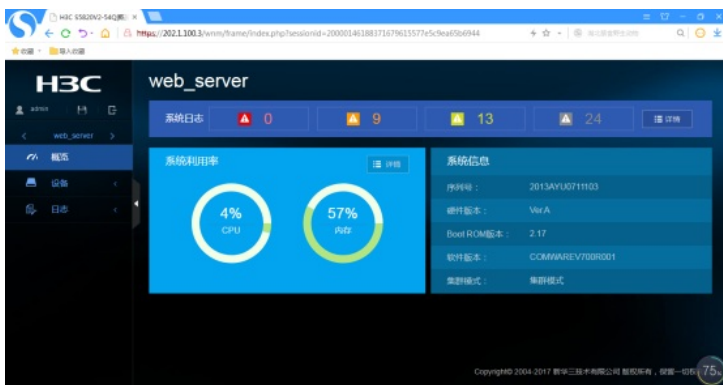
物理机打开浏览器，输入网址：<https://202.1.100.3>，可以登陆到web服务器



输入用户名、密码，点击登录：



登陆成功：



查看FW1 NAT的显示信息：

```
[FW1]dis nat server
NAT internal server information:
Totally 2 internal servers.
Interface: GigabitEthernet1/0/4
  Protocol: 6(TCP)
  Global IP/port: 202.1.100.3/80
  Local IP/port : 10.0.0.2/80
  NAT counting : 0
  Config status : Active

Interface: GigabitEthernet1/0/4
  Protocol: 6(TCP)
  Global IP/port: 202.1.100.3/443
  Local IP/port : 10.0.0.2/443
  NAT counting : 0
  Config status : Active

[FW1]
```

```
[FW1]dis nat session
Slot 1:
Initiator:
  Source      IP/port: 202.103.224.68/50795
  Destination IP/port: 202.1.100.3/443
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/4
  Source security zone: Untrust

Initiator:
  Source      IP/port: 202.103.224.68/50800
  Destination IP/port: 202.1.100.3/443
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/4
  Source security zone: Untrust

Initiator:
  Source      IP/port: 202.103.224.68/50798
  Destination IP/port: 202.1.100.3/443
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/4
  Source security zone: Untrust

Total sessions found: 3
[FW1]
```

```
[FW1]dis nat outbound
NAT outbound information:
Totally 1 NAT outbound rules.
Interface: GigabitEthernet1/0/4
  ACL: 2000
  Address group ID: ---
  Port-preserved: N      NO-PAT: N  Reversible: N
  NAT counting: 0
  Config status: Active

[FW1]
```

[FW1]dis nat session verbose

Slot 1:

Total sessions found: 0

[FW1]dis nat session verbose

Slot 1:

Initiator:

Source IP/port: 202.103.224.68/50855

Destination IP/port: 202.1.100.3/443

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/

Protocol: TCP(6)

Inbound interface: GigabitEthernet1/0/4

Source security zone: Untrust

Responder:

Source IP/port: 10.0.0.2/443

Destination IP/port: 202.103.224.68/50855

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/

Protocol: TCP(6)

Inbound interface: GigabitEthernet1/0/3

Source security zone: Trust

State: TCP_ESTABLISHED

Application: HTTPS
Rule ID: 0
Rule name:
Start time: 2020-03-07 10:34:53 TTL: 596s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0 bytes

Initiator:
Source IP/port: 202.103.224.68/50853
Destination IP/port: 202.1.100.3/443
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/4
Source security zone: Untrust

Responder:
Source IP/port: 10.0.0.2/443
Destination IP/port: 202.103.224.68/50853
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/3
Source security zone: Trust

State: TCP_ESTABLISHED

Application: HTTPS
Rule ID: 0
Rule name:
Start time: 2020-03-07 10:34:52 TTL: 596s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0 bytes

Initiator:
Source IP/port: 202.103.224.68/50860
Destination IP/port: 202.1.100.3/443
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/4
Source security zone: Untrust

Responder:
Source IP/port: 10.0.0.2/443
Destination IP/port: 202.103.224.68/50860
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/3
Source security zone: Trust

State: TCP_ESTABLISHED

Application: HTTPS
Rule ID: 0
Rule name:
Start time: 2020-03-07 10:34:53 TTL: 596s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0 bytes

Initiator:
Source IP/port: 202.103.224.68/50852
Destination IP/port: 202.1.100.3/443
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/4
Source security zone: Untrust

Responder:

Source IP/port: 10.0.0.2/443
Destination IP/port: 202.103.224.68/50852
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/3
Source security zone: Trust
State: TCP_ESTABLISHED
Application: HTTPS
Rule ID: 0
Rule name:
Start time: 2020-03-07 10:34:52 TTL: 596s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0 bytes

Initiator:

Source IP/port: 202.103.224.68/50861
Destination IP/port: 202.1.100.3/443
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/4
Source security zone: Untrust

Responder:

Source IP/port: 10.0.0.2/443
Destination IP/port: 202.103.224.68/50861
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/3
Source security zone: Trust
State: TCP_ESTABLISHED

Application: HTTPS

Rule ID: 0

Rule name:

Start time: 2020-03-07 10:34:53 TTL: 597s

Initiator->Responder: 0 packets 0 bytes

Responder->Initiator: 0 packets 0 bytes

Initiator:

Source IP/port: 202.103.224.68/50859
Destination IP/port: 202.1.100.3/443
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/4
Source security zone: Untrust

Responder:

Source IP/port: 10.0.0.2/443
Destination IP/port: 202.103.224.68/50859
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/3
Source security zone: Trust
State: TCP_ESTABLISHED

Application: HTTPS

Rule ID: 0

Rule name:

Start time: 2020-03-07 10:34:53 TTL: 597s

Initiator->Responder: 0 packets 0 bytes

Responder->Initiator: 0 packets 0 bytes

Total sessions found: 6

[FW1]

至此，F1060 NAT server典型组网配置案例1（有固定公网IP地址转换）已完成！