

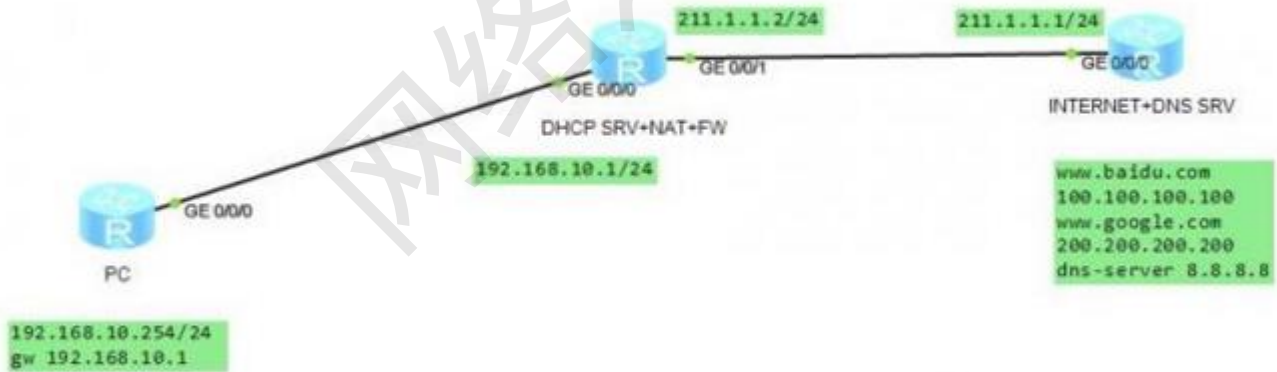
华为路由交换由浅入深系列（十二）：ENSP2.0 模拟 NAT+Firewall+DNS+DHCP 功能

ENSP2.0 模拟 NAT+Firewall+DNS+DHCP 功能，主要涉及在华为路由器上面，如何实现防火墙特性、NAT、DNS、DHCP 功能。

掌握目标

- 1、路由器 DHCP 客户端配置（模拟 PC）
- 2、防火墙特性配置
- 3、NAT 配置
- 4、DNS 与 DHCP 的配置掌握

一、实验拓扑：



二、PC 的配置

```
#
```

```
sysname PC
```

```
dhcp enable
```

```
dns resolve
```

```
dns server 8.8.8.8
```

```
#
```

```
interface GigabitEthernet0/0/0
```

```
ip address dhcp-alloc
```

三、网关路由器的配置

```
#
```

```
sysname GW
```

```
#
```

```
dhcp enable
```

```
dns resolve
```

```
dns server 8.8.8.8
```

```
#
```

```
acl number 3000
```

```
rule 5 permit ip source 192.168.10.0 0.0.0.255
```

```
acl number 3001
```

```
rule 5 deny icmp icmp-type echo
```

```
rule 10 permit ip
```

```
#
```

```
firewall zone trust
```

```
priority 10
```

#

firewall zone untrust

priority 5

#

firewall zone Local

priority 15

#

firewall interzone trust untrust

firewall enable

packet-filter 3001 inbound

detect aspf ftp

detect aspf sip

detect aspf rtsp

detect aspf http

detect aspf http java-blocking

detect aspf http activex-blocking

#

interface GigabitEthernet0/0/0

ip address 192.168.10.1 255.255.255.0

zone trust

dhcp select interface

dhcp server dns-list 8.8.8.8

```
#  
interface GigabitEthernet0/0/1  
ip address 211.1.1.2 255.255.255.0  
nat outbound 3000  
zone untrust  
#  
ip route-static 0.0.0.0 0.0.0.0 GigabitEthernet0/0/1 211.1.1.1  
#  
user-interface vty 0 4  
authentication-mode password  
set authentication password cipher huawei  
user privilege level 3
```

四、公网路由器的配置

```
#  
sysname INTERNET  
#  
ip host www.baidu.com 100.100.100.100  
ip host www.google.com 200.200.200.200  
#  
dns resolve  
dns server 8.8.8.8
```

```
dns proxy enable
#
interface GigabitEthernet0/0/0
ip address 211.1.1.1 255.255.255.0
#
interface NULL0
#
interface LoopBack0
ip address 100.100.100.100 255.255.255.0
#
interface LoopBack1
ip address 200.200.200.200 255.255.255.0
#
interface LoopBack100
ip address 8.8.8.8 255.255.255.0
#
user-interface vty 0 4
authentication-mode password
set authentication password cipher huawei
user privilege level 3
#
```

五、测试 PC 上网

<PC>ping www.google.com

PING www.google.com: 56 data bytes, press CTRL_C to break

Reply from 200.200.200.200: bytes=56 Sequence=1 ttl=254 time=20 ms

Reply from 200.200.200.200: bytes=56 Sequence=2 ttl=254 time=20 ms

Reply from 200.200.200.200: bytes=56 Sequence=3 ttl=254 time=10 ms

Reply from 200.200.200.200: bytes=56 Sequence=4 ttl=254 time=10 ms

Reply from 200.200.200.200: bytes=56 Sequence=5 ttl=254 time=30 ms

--- www.google.com ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 10/18/30 ms

<PC>telnet www.baidu.com

Press CTRL_] to quit telnet mode

Trying 100.100.100.100 ...

Connected to 100.100.100.100 ...

Login authentication

Password:huawei

<INTERNET>dis access-user

Info: No online user.

<INTERNET>dis ip inter bri

*down: administratively down

^down: standby

(l): loopback

(s): spoofing

The number of interface that is UP in Physical is 5

The number of interface that is DOWN in Physical is 1

The number of interface that is UP in Protocol is 5

The number of interface that is DOWN in Protocol is 1

Interface	IP Address/Mask	Physical	Protocol
GigabitEthernet0/0/0	211.1.1.1/24	up	up
GigabitEthernet0/0/1	unassigned	down	down
LoopBack0	100.100.100.100/24	up	up(s)
LoopBack1	200.200.200.200/24	up	up(s)
LoopBack100	8.8.8.8/24	up	up(s)
NULL0	unassigned	up	up(s)
<INTERNET>			

六、测试网关的状态

[GW]dis nat session all

NAT Session Table Information:

Protocol : ICMP(1)

SrcAddr Vpn : 192.168.10.254

DestAddr Vpn : 200.200.200.200

Type Code IcmpId : 0 8 43997

NAT-Info

New SrcAddr : 211.1.1.2

New DestAddr : ----

New IcmpId : 10255

Protocol : TCP(6)

SrcAddr Port Vpn : 192.168.10.254 46273

DestAddr Port Vpn : 100.100.100.100 5888

NAT-Info

New SrcAddr : 211.1.1.2

New SrcPort : 10253

New DestAddr : ----

New DestPort : ----

Protocol : UDP(17)

SrcAddr Port Vpn : 192.168.10.254 7109

DestAddr Port Vpn : 8.8.8.8 13568

NAT-Info

[GW]dis firewall session all

Firewall Session Table Information:

Protocol : TCP(6)

SrcAddr Port Vpn : 192.168.10.254 46273

DestAddr Port Vpn : 100.100.100.100 5888

Firewall-Info

InZone : trust

OutZone : untrust

Protocol : UDP(17)

SrcAddr Port Vpn : 192.168.10.254 7109

DestAddr Port Vpn : 8.8.8.8 13568

Firewall-Info

InZone : trust

OutZone : untrust

Protocol : UDP(17)

SrcAddr Port Vpn : 192.168.10.254 2245

DestAddr Port Vpn : 8.8.8.8 13568

Firewall-Info

InZone : trust

OutZone : untrust

Protocol : UDP(17)

SrcAddr Port Vpn : 192.168.10.254 33990

DestAddr Port Vpn : 8.8.8.8 13568

Firewall-Info

InZone : trust

OutZone : untrust
Protocol : UDP(17)
SrcAddr Port Vpn : 192.168.10.254 4806
DestAddr Port Vpn : 8.8.8.8 13568

Firewall-Info

InZone : trust
OutZone : untrust
Protocol : UDP(17)
SrcAddr Port Vpn : 192.168.10.254 4038
DestAddr Port Vpn : 8.8.8.8 13568

Firewall-Info

InZone : trust
OutZone : untrust
Protocol : TCP(6)
SrcAddr Port Vpn : 192.168.10.254 21700
DestAddr Port Vpn : 100.100.100.100 5888

Firewall-Info

博主也只是业余时间写写技术文档，请大家见谅，大家觉得不错的话，可以推荐给朋友哦，博主会努力推出更好的系列文档的。如果大家有任何疑问或者文中有错误跟疏忽的地方，欢迎大家留言指出，博主看到后会第一时间修改，谢谢大家的支持，更多技术文章尽在网络之路博客，<http://ccieh3c.com>。