ELEC 5220/6220 Information Networks and Technology  
LAB 11 REPORT

George Gavin Conover, Jie Zou, Ningkai Tang, Olufeni Anuolupo Okelana, Sushma Reddy R Kondapally, Xiao Lin

# Abstract

In this lab we are going to configure a router and set up a firewall. This router will be set with a DMZ which will allow private network to access internet as well as the outside server however this will outside client access internal server in DMZ. In the first we should configure the router with interfaces for different subnets. And when we set up the fire wall, we should make some special functions which will filter informations from or deliver to certain IP address. And in total, we should also to prove these subnets we set up can be manipulated by our router's settings.

# Introduction

In this lab we will have three subnet in total, they are: one DMZ subnet whose address will be 192.168.127.0/24, one public subnet 131.204.128.0/24 and one private subnet 10.10.10.0/24.

In this lab the router we use is the ADTRAN NetVanta3120. This router will give us interconnections as well as the management of network traffic within these subnets.

The public subnet(131.204.128.0/24) is connected to the eth0/1 port which is the public port of router. the private subnet(10.10.10.0/24) and DMZ subnet are separated into two different VLAN and they are connected to the router by the internal ports(port 0 and port 1). After setting the configuration of firewall, NAPT rules and security zones, the router will give these VLAN access to internet through NAPT. And it will also allow internet to access DMZ server. And all the other access will be denied by router.

In this lab, we use three computers to finish it. Our three computers will be refereed to as A,B,C as shown in the table below:

|  |  |  |
| --- | --- | --- |
| **IP Address** | **Computer Alias** | **Operating System** |
| **131.204.128.2** | A | Windows 7 |
| **192.168.127.2** | B | Windows 7 |
| **10.10.10.2** | C | MAC OS |

# Design

## Bind 9

First we download BIND9 at [www.isc.org](http://www.isc.org) and then install it.

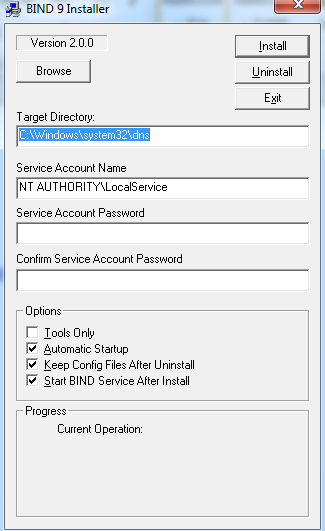


Figure Install BIND9

We find the service account name at the readme.txt file.

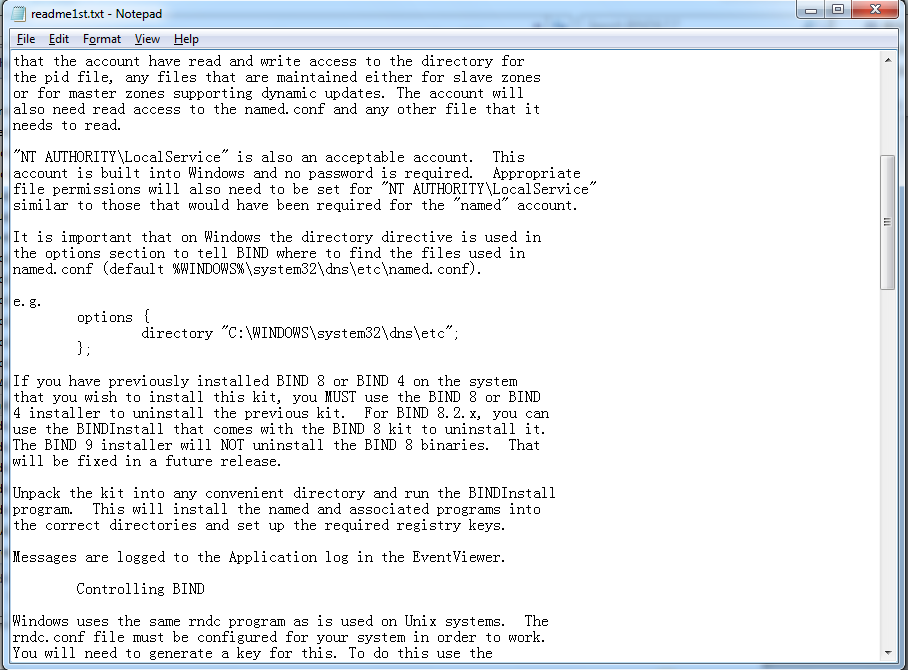


Figure service account name

Then we create master.localhost, localhost.rev, named.conf and root.servers files in the C:\Windows\System32\dns\etc for windows 7 32 bit version.

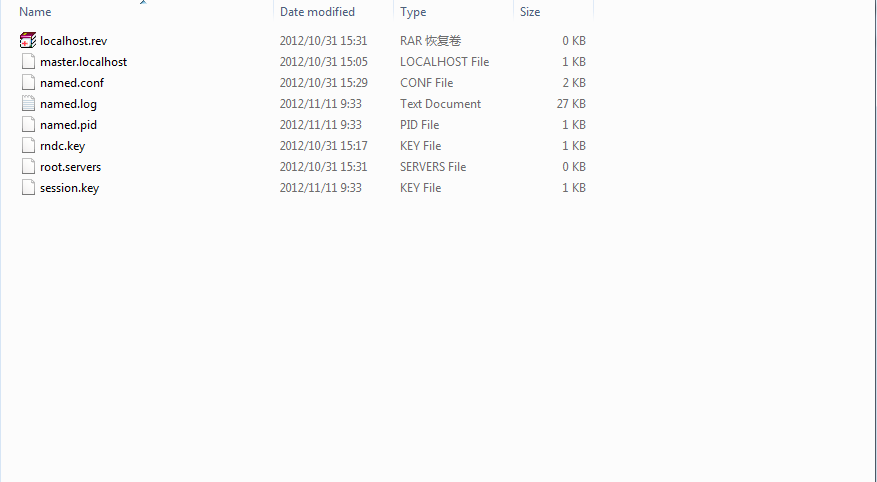


Figure create files

Then enable user account of windows all authority for dns.

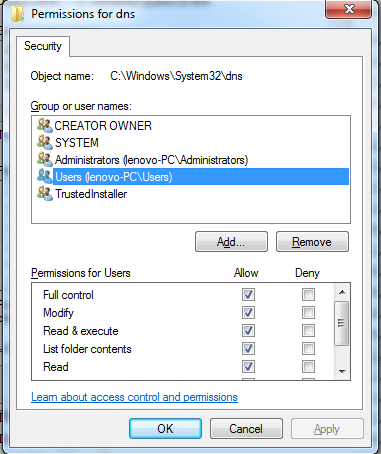


Figure Enable authority

Next we need to add the rndc key file to the etc folder. In the cmd window, go the the directory C:\Windows\System32\dns\etc and then type rndc-confgen –a.

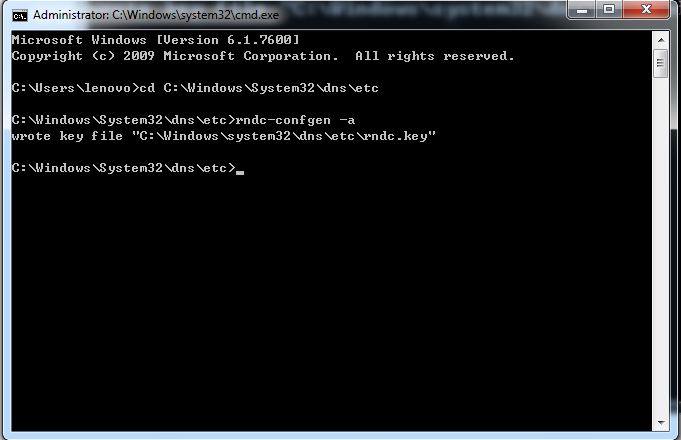


Figure Create rndc key file

Go the administrative tool, choose service and edit DNS Client’s properties. Select Manual and stop the service.

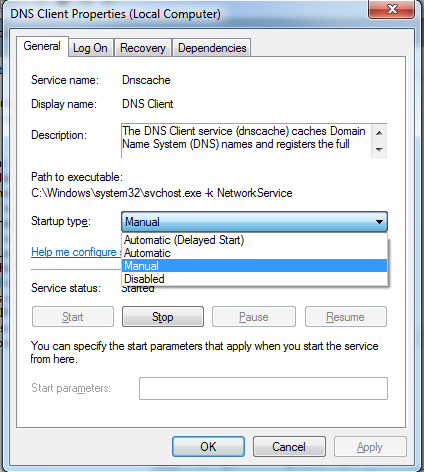


Figure DNS Client properties

Then start ISC BIND service.

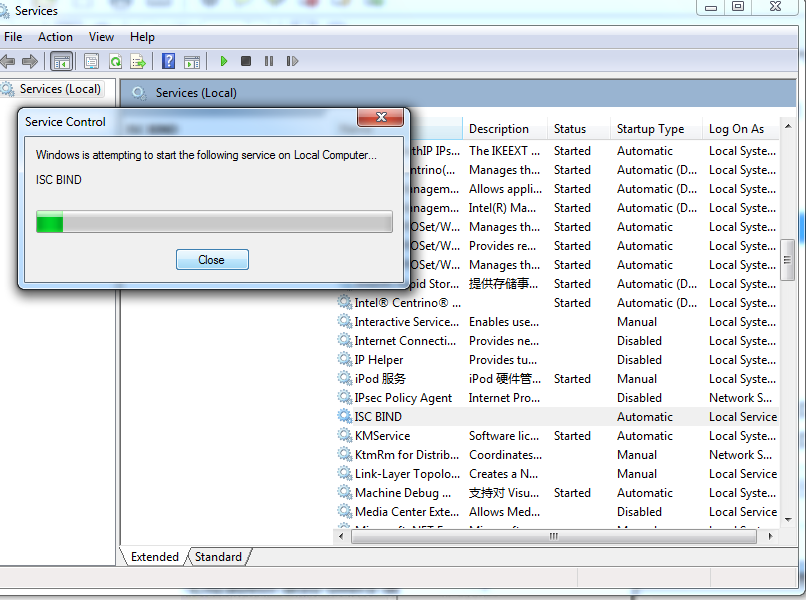
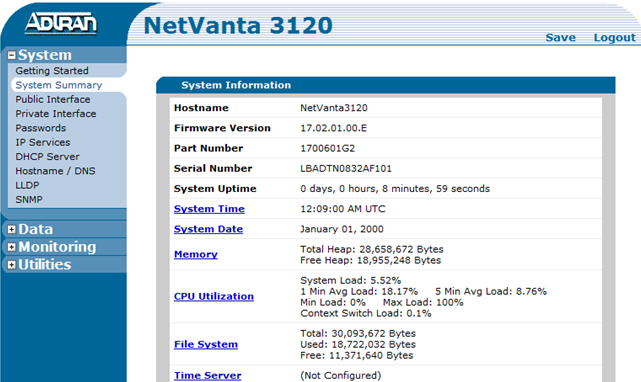


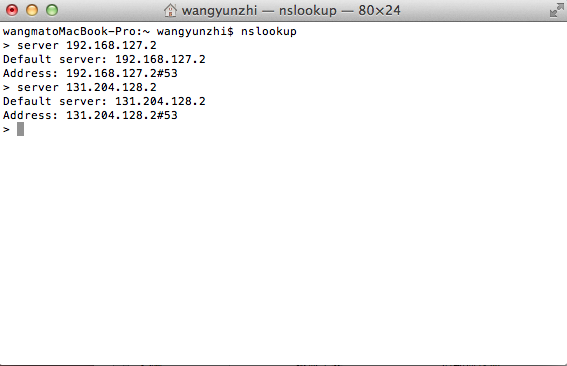
Figure Starting ISC BIND service

## Step 1: use two servers that each performs both Web and DNS server: one @ 192.168.127.2 and the other @ 131.204.128.2

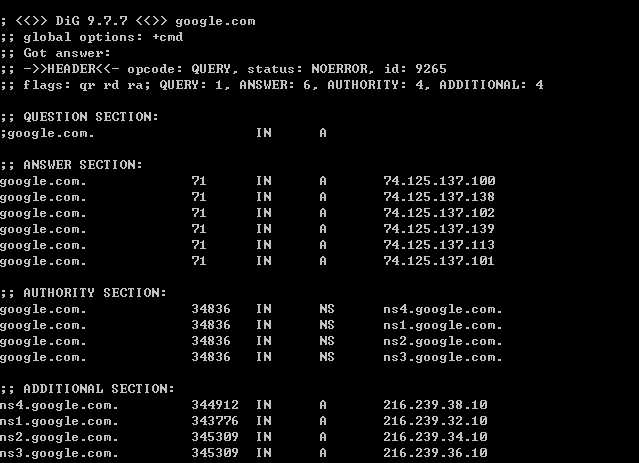
After installing BIND service, we have to restore the settings to factory default:



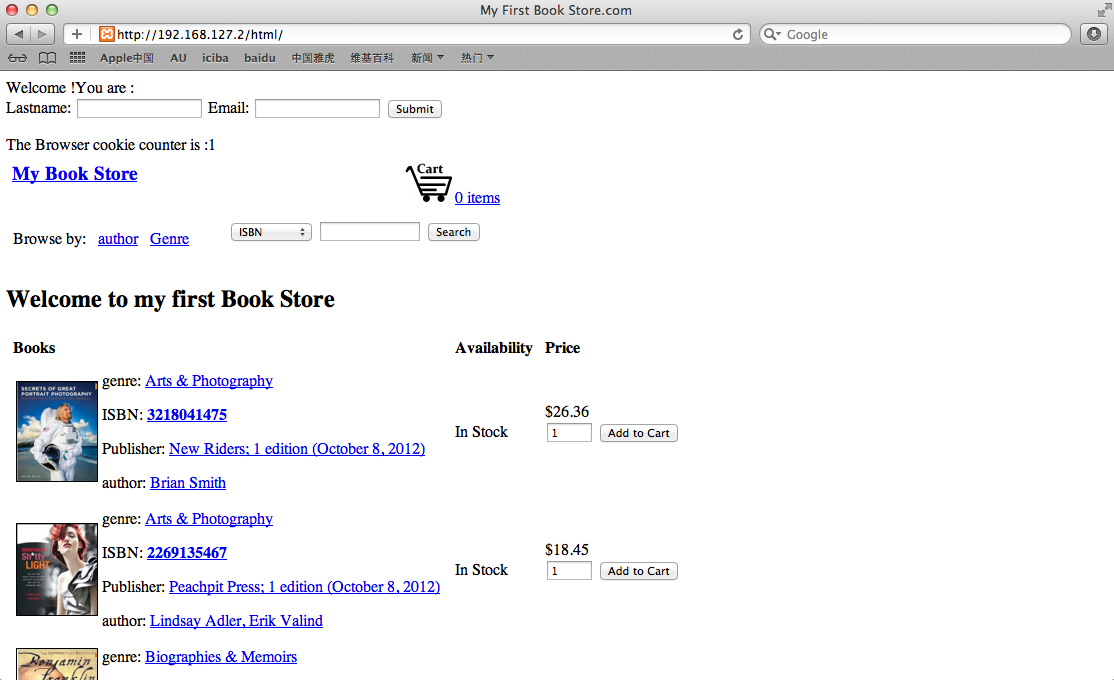
Then let`s see the if the DNS is working well:

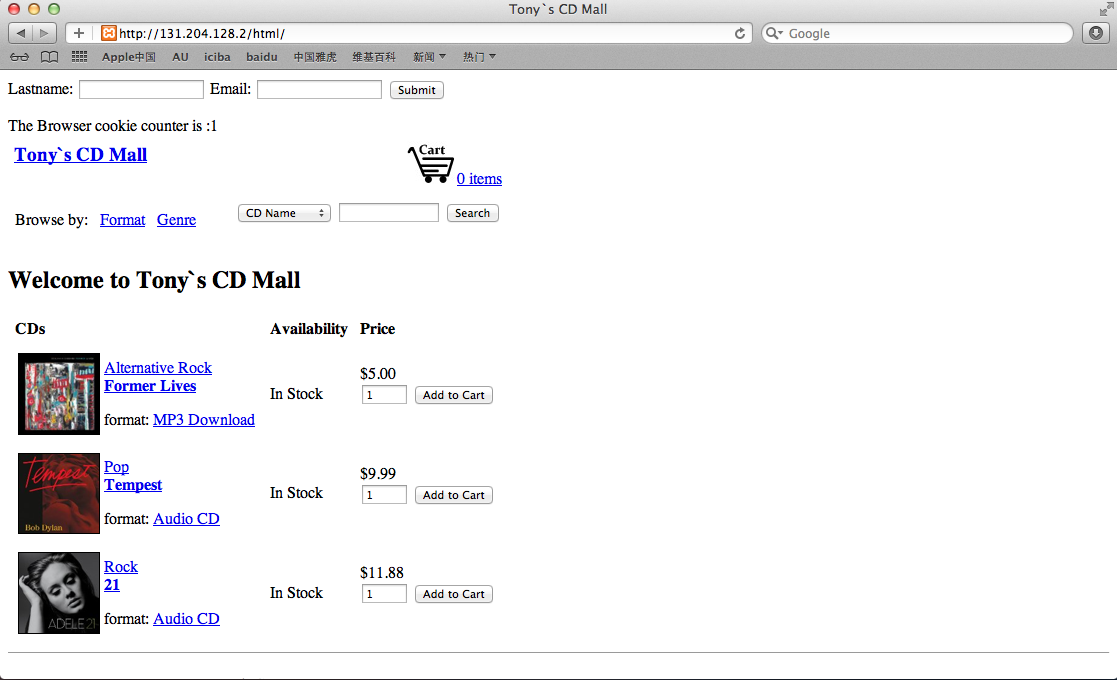


And the dig result from DNS server:



To prove the web server is working well, let`s access web server from 10.10.10.2 to both 131.204.128.2 and 192.168.127.2:

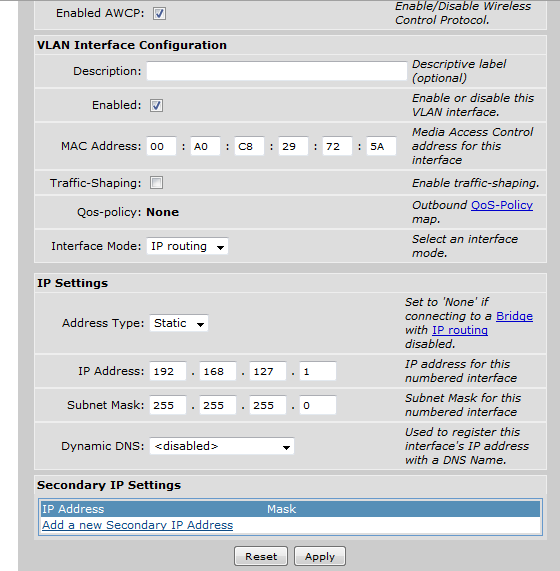




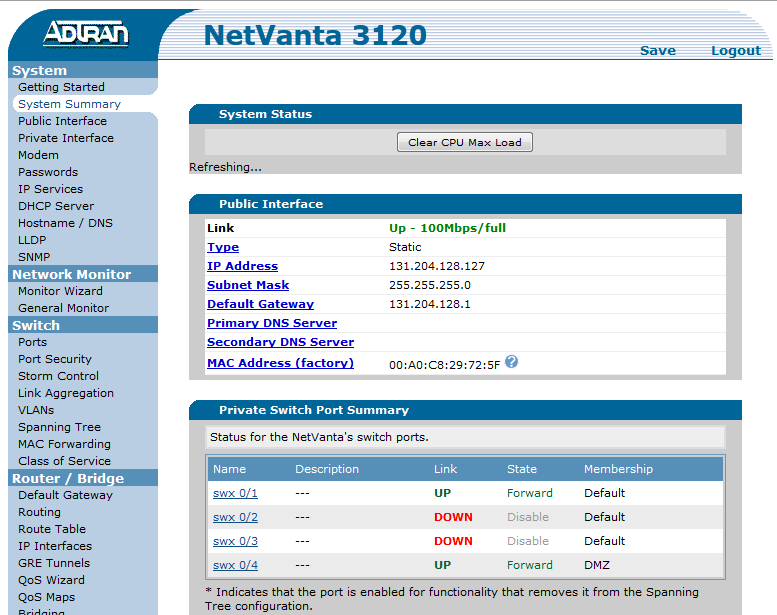
We can see they`re functioning well.

## Step 2: Establish routing between 3 subnets: 131.204.128.0/24, 192.168.127.0/24, 10.10.10.0/24.

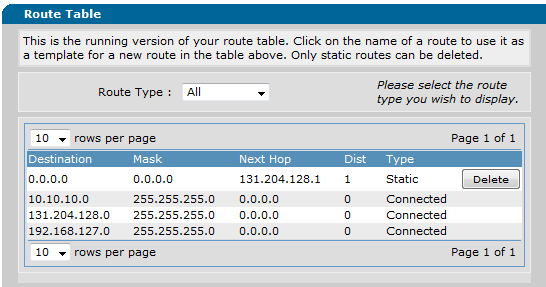
To establish routing between different subnets, we have to set VLAN first:



After the DMZ VLAN, we`re going to get public interface done and assign the exact port to certain VLANs, like below:

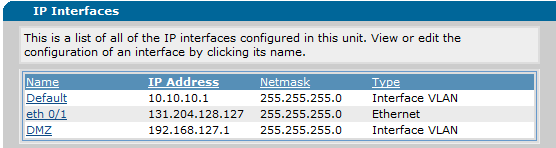


Now let`s check the routing table to see if it`s done:



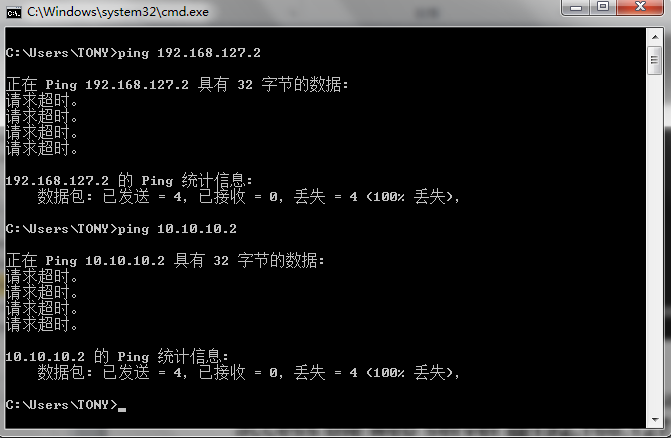
Nothing wrong with the table.

And the interfaces:

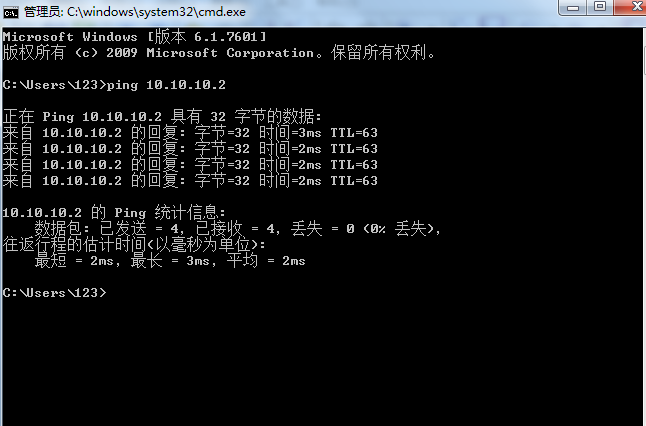


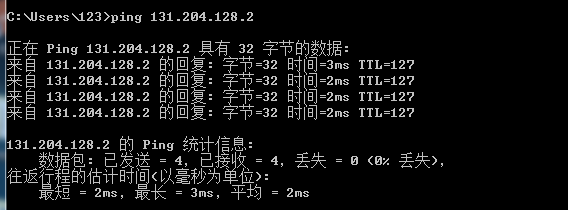
Now let`s check it by the practical ping command:

For 131.204.128.2



For 192.168.127.2:

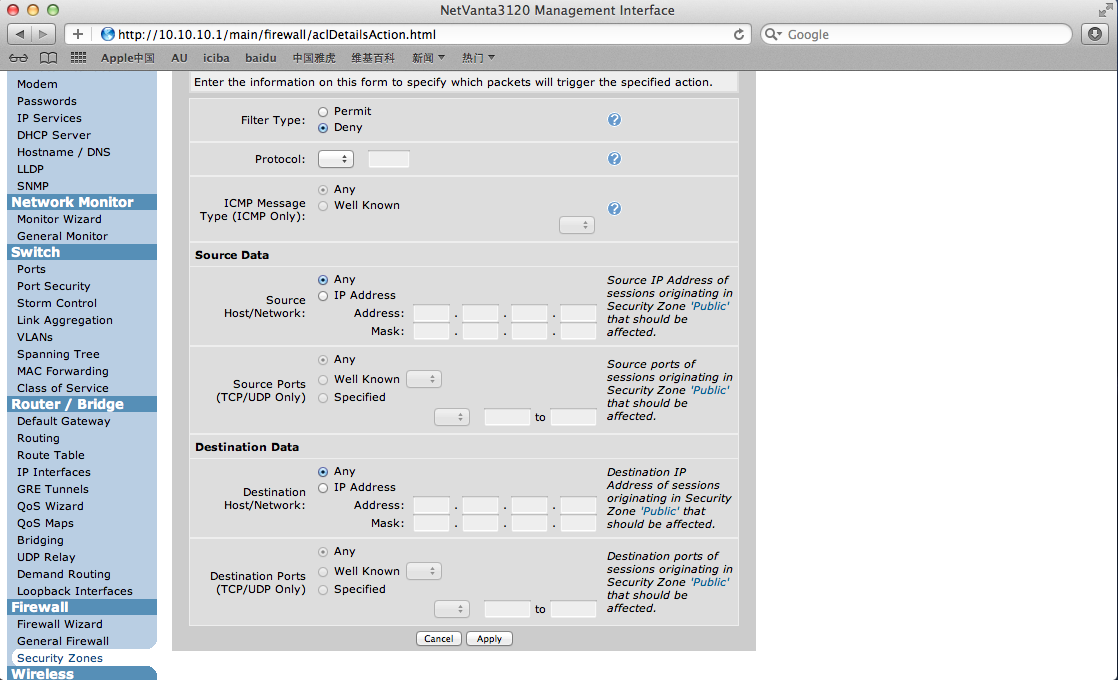




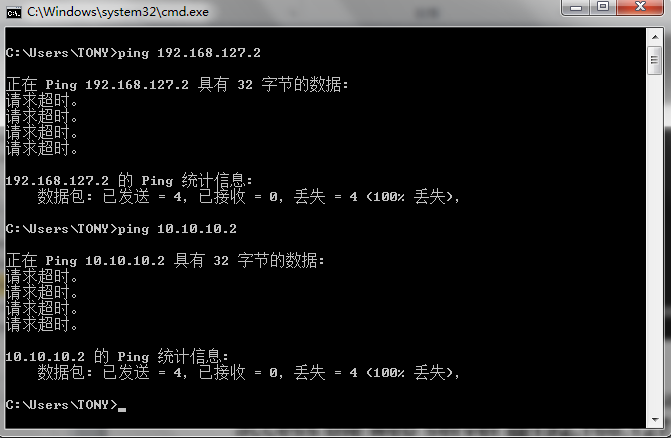
So we can see they can reach each other subnets.

## Step 3: Establish a firewall so that only the two inside subnets can read 131.204.128.2 but outside subnet cannot read 192.168.127.2

To achieve the goal, we can set public security zone with a ACL that prevent any public access from reaching private zone:



Let`s use ping command to make a test:

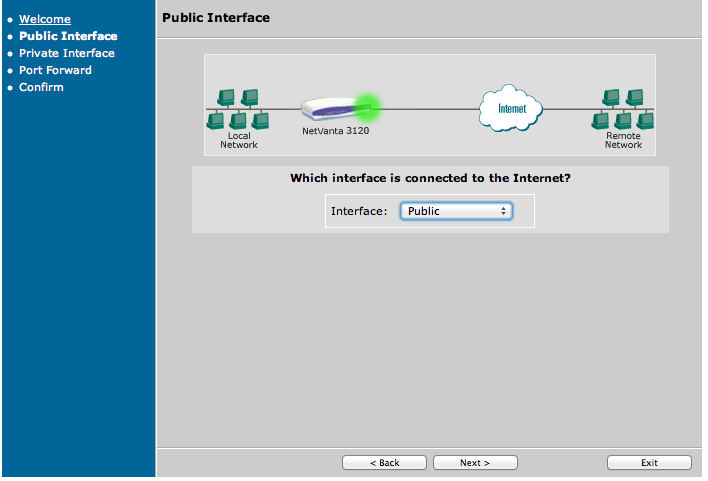


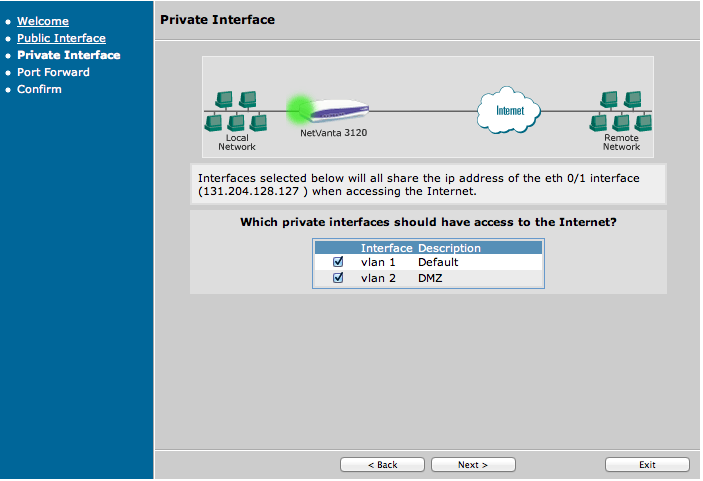
The policy works well.

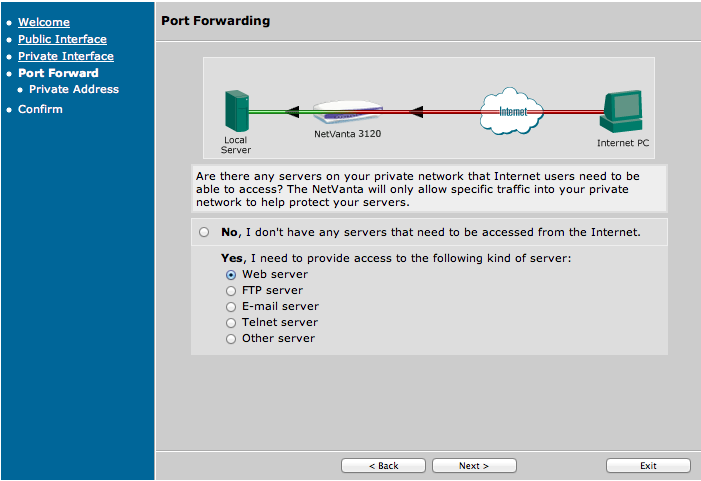
## Step 4: Punch a hole in the firewall so that outside computer can access the web server@192.168.127.2. The NAPT lets the DMZ web server have the outside IP address of 131.204.128.127

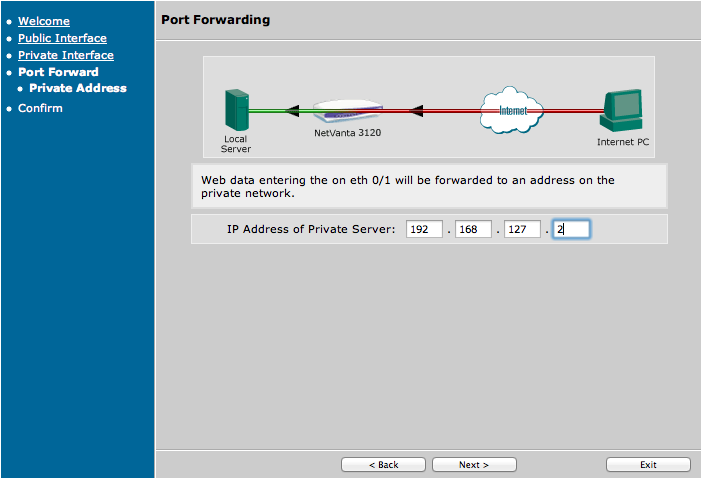
We can use firewall wizard to realize the needing:

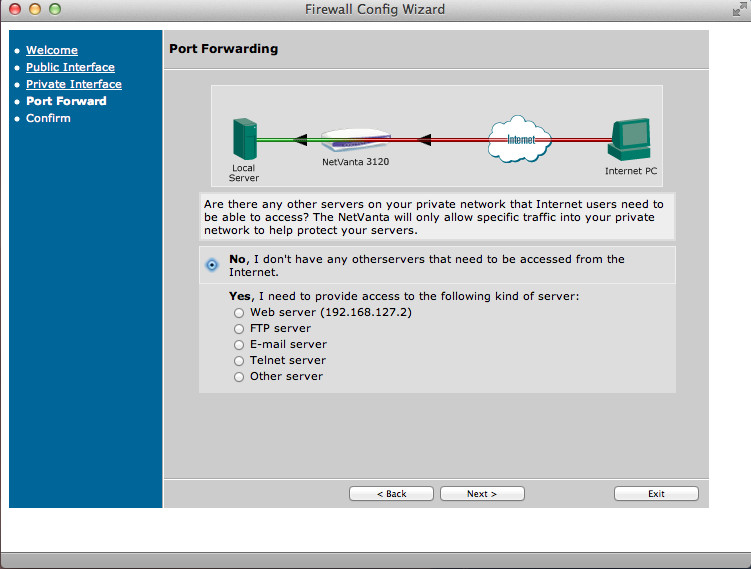
Just follow my screenshot and we can make the tunnel come true:

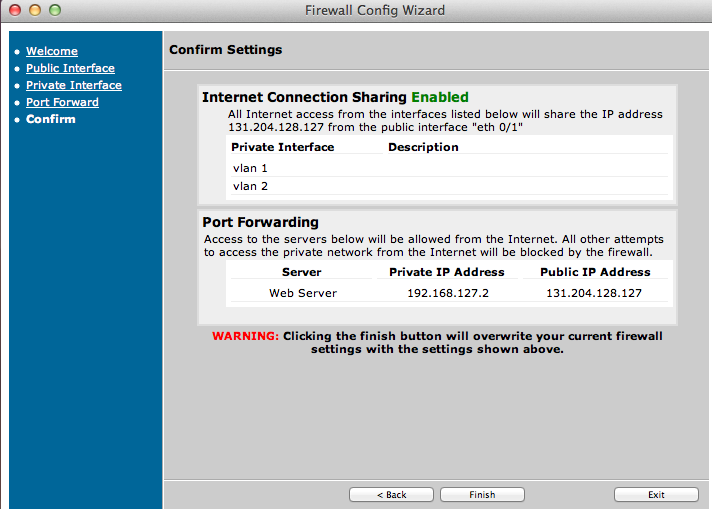




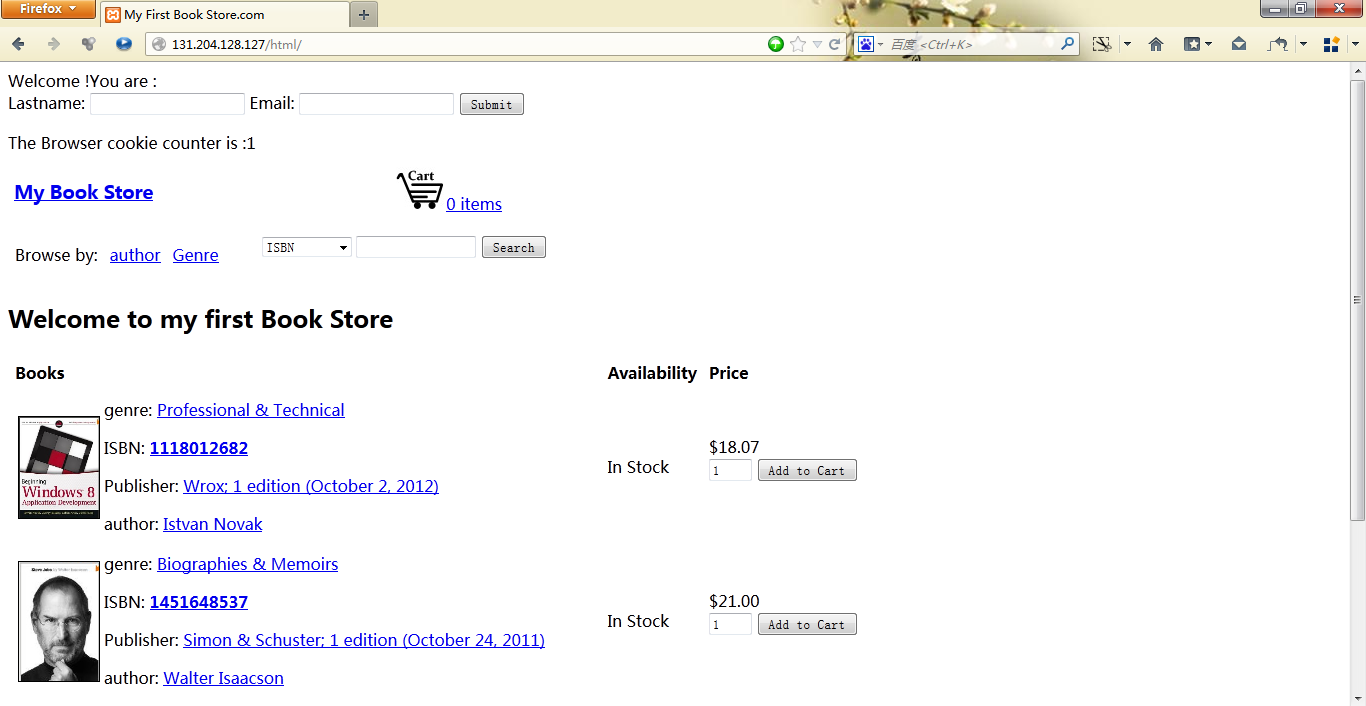




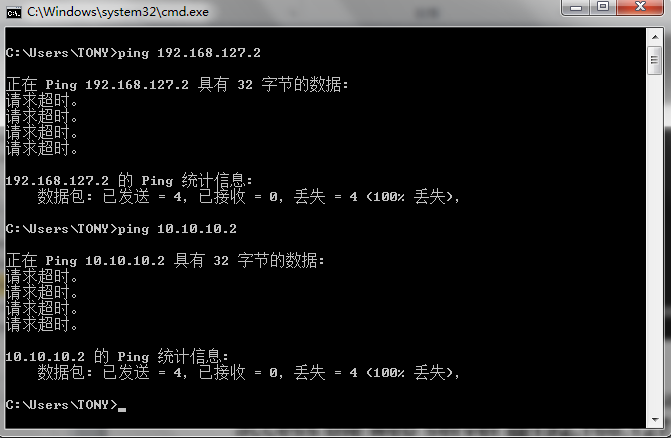




Now we can access 192.168.127.2`s web service by accessing the alias of 131.204.128.127:

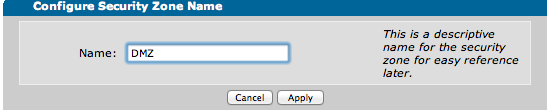


And we cannot access any of the private subnet with their true IP still:

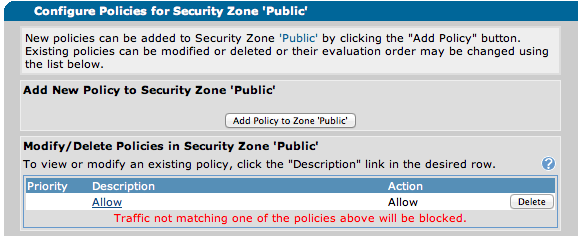


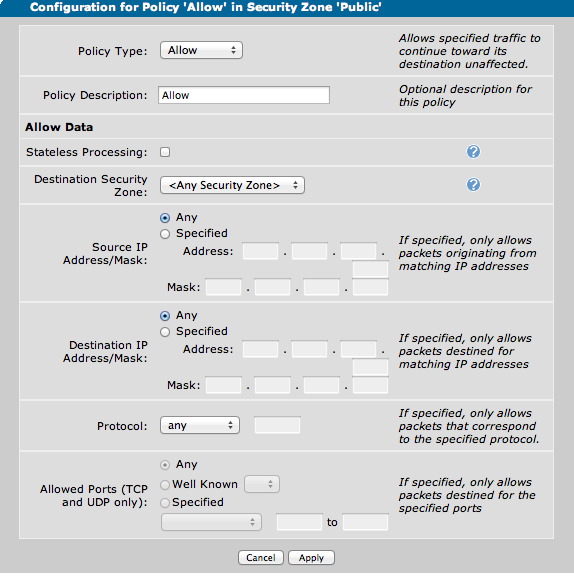
## Step 5: Establish the DMZ so that both the outside (131.204.128.2) and inside (10.10.10.0) can access 192.168.127.2; however the 192.168.127.2 cannot access 10.10.10.0. Both 10.10.10.0 and 192.168.127.0/24 can access 131.204.128.2

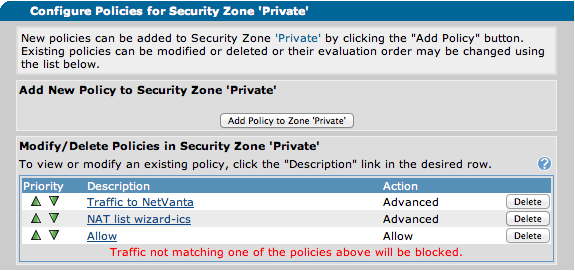
Let`s assign a new security zone named DMZ to set private policy, then assign the new DMZ security zone to DMZ:

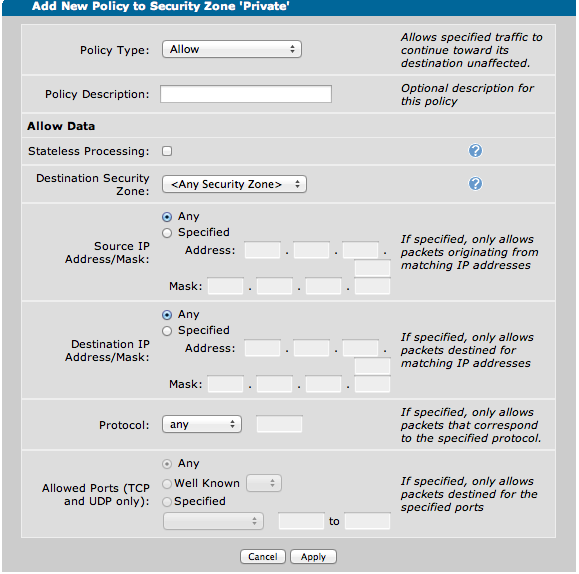


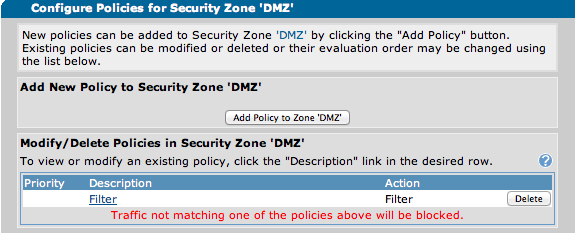
Then let`s define each zone with their security policy:

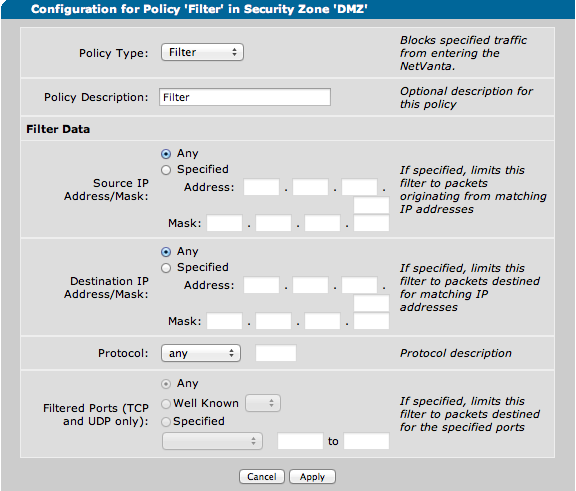




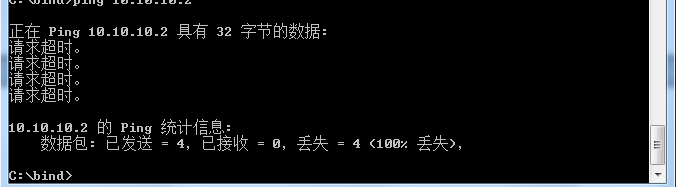






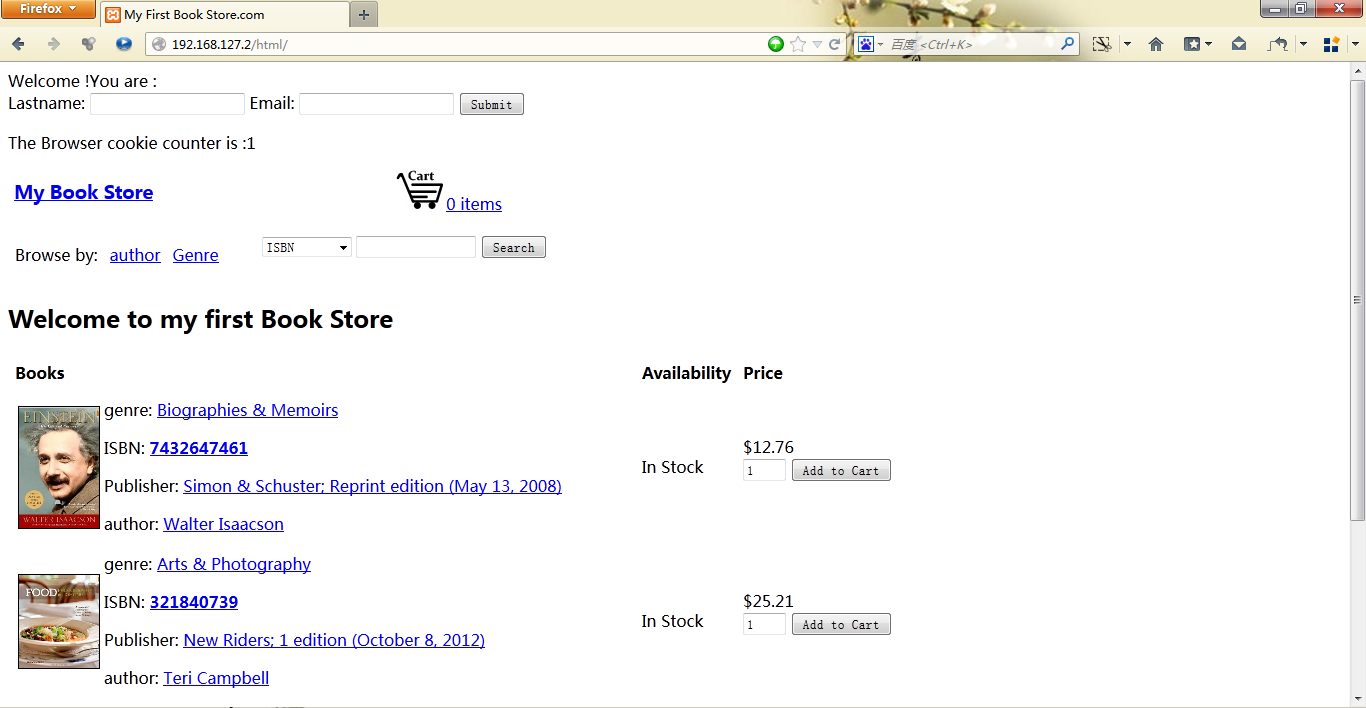


Now let`s test if it works:

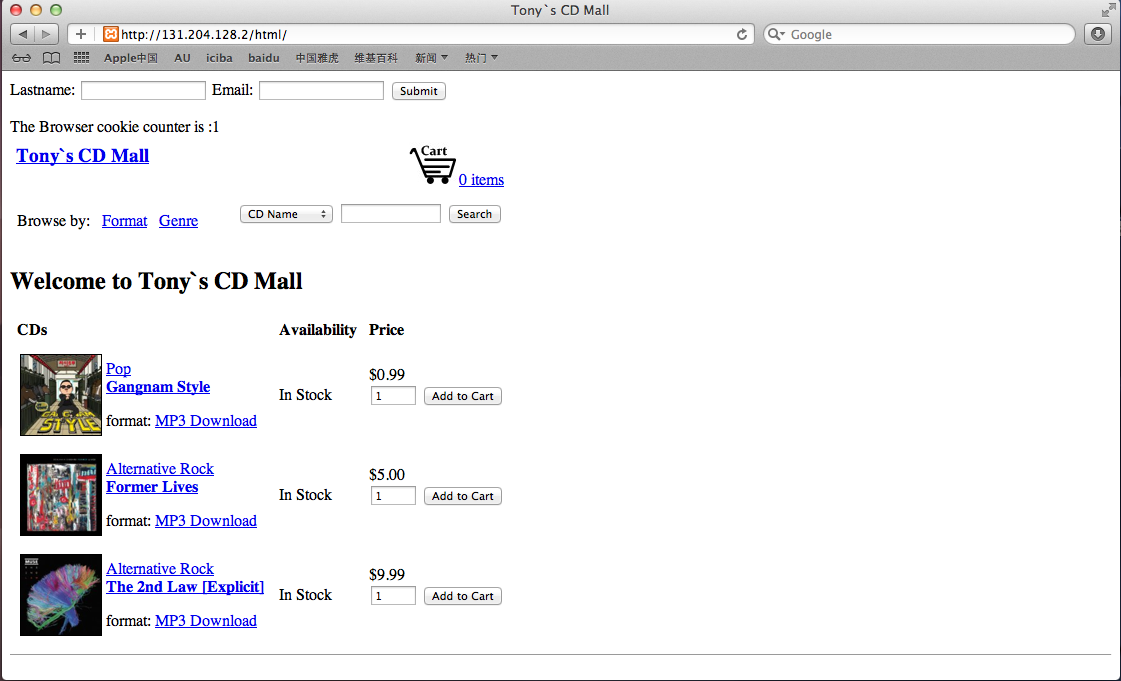


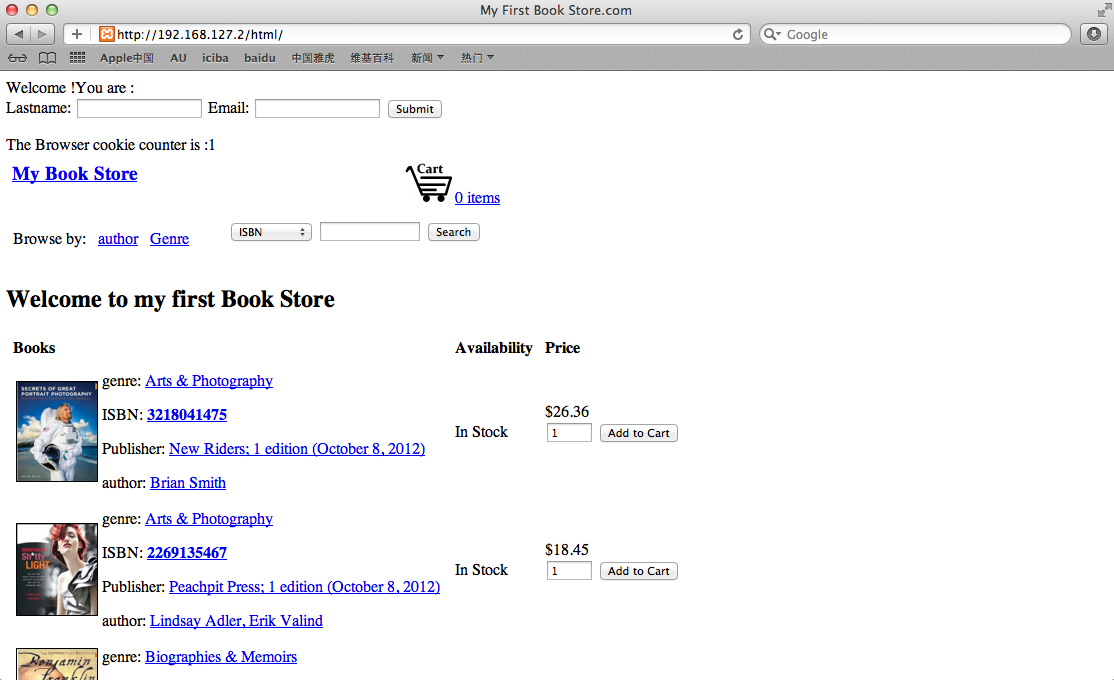


192.168.127.2 cannot reach 10.10.10.2 now.



131.204.128.2 is still able to access 192.168.127.2.





And 10.10.10.2 is still fine with every site, thus the policy is performing well.

# Result

In this lab we have complete all step without significant problems. Through all of the exercises in this lab we have gain a understanding of how to configure network router with firewall as well as different security zones. Besides we also have learn how to setup subnet with NAPT and the local DMZ. In this lab the last two steps are a little difficult, but we work together and solve the problems.

# Conclusion

This lab is very informative and useful.

We are all very satisfied with exercise of practicing router configuration and network setting. It gives us deeper understanding of the network and routing issues.

# References

* ADTRAN NetVanta 3120 router, <http://www.adtran.com/web/page/portal/Adtran/product/1700601G2/117>
* Dr.Wu's lab guide
* Mr.Hou's slides for lab