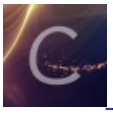
Linux实验精华总结

转载

硬核的无脸man~ 于 2018-01-29 13:30:09 发布 9109 收藏 10
分类专栏： Linux运维 在校所学知识整理 文章标签： Linux实验精华总结
原文链接：https://blog.csdn.net/Until_U/article/details/79193327
版权


Linux运维 同时被 2 个专栏收录
14 篇文章 1 订阅
订阅专栏


在校所学知识整理
18 篇文章 33 订阅
订阅专栏

目录

一、 配置yum本地源

#mkdir /media/cdrom

#mount /dev/cdrom /media/cdrom

cd /etc/yum.repos.d

#mkdir bak

#ll

#mv CentOS-base.repo CentOS-Debuginfo.repo CentOS-Vault.repo bak

#gedit CentOS-Media.repo

把0改为1

#yum clean all

#yum makecache

二、基础网络搭建

#gedit /etc/udev/rules.d/70-persistent-net.rules

(前三个网卡信息删掉接着吧eth3改为eth0并且把物理地址复制下来)

#gedit /etc/sysconfig/network-scripts/ifcfg-eth0

（把DHCP改为static并且添加ip地址，子网掩码，网关）

如：IPADDR=192.168.0.10

NETMASK=255.255.255.0

GATEWAY=192.168.0.254

开启转发：

#gedit /etc/sysctl.conf

(net.ipv4.ip forward=0中把0改为1)

#sysctl -p

#service iptables stop

三、内网访问外网web

基础网络搭建，然后在外网和网关上防火墙放行。

外网：

[root@lyyyum.repos.d]# iptables -A INPUT -i eth1 -p tcp --dport 80 -j ACCEPT

[root@lyyyum.repos.d]# iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

[root@lyyyum.repos.d]# iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT

网关：

iptables -A FORWARD -d202.3.4.10/32 -i eth0 -o eth1 -p tcp -m tcp --dport 80 -j ACCEPT

iptables -A FORWARD -s202.3.4.10/32 -m state --state RELATED,ESTABLISHED -j ACCEPT

四、 防火墙3——SNAT1

在访问web基础上做下面：

然后在网关防火墙上设置SNAT

#iptables –t nat –A POSTROUTING –s 192.168.0.0/24 –o eth1–j MASQUERADE

MASQUERADE:动态地址伪装，用发送数据的网卡上的IP来替换源IP

五、安装vnc 远程控制

1、Vnc-server：安装yum,

#yum installtigervnc-server –y

#vncserver //(设置一下密码，还要重新确认一下,注意下主机号是1还是2))

#iptables-save //查看规则

#iptables –IINPUT –p tcp –m state ——state NEW –m tcp ——dport 5801 –j ACCEPT

#iptables –IINPUT –p tcp –m state ——state NEW –m tcp ——dport 5901 –j ACCEPT

//添加规则

#iptables-save //查看规则

1、 vnc-client：安装yum

#yum install tigervnc –y

然后直接可以运行软件了

六、nfs服务器的搭建

1、 配置ip，设置网卡。不做说明：

然后安装nfs服务器，默认已经安装好。

```
1  gedit /etc/udev/rules.d/70-persistent-net.rules
2  gedit /etc/sysconfig/network-scripts/ifcfg-eth0
3  shutdown -r now
4  ping 192.168.0.9
5  mkdir /tmp/test1 /tmp/test2
6  ll /tmp
7  touch /tmp/test1/a1
8  touch /tmp/test2/b1
9  chmod a+x /tmp/test1
10 gedit /etc/export
11 gedit /etc/exports
12 cat /etc/exports
13 gedit
14 gedit /etc/sysconfig/nfs
15 service nfs start
16 history
```

http://blog.csdn.net/Until_U

exports

```
/tmp/test1 192.168.0.0/24(rw,sync)
/tmp/test2 192.168.0.9(rw,sync)
```

http://blog.csdn.net/Until_U

将/etc/sysconfig/nfs 文件中（875 32803 32769 892）前面#删掉

```
[root@localhost 桌面]# showmount -e localhost
Export list for localhost:
/tmp/test2 192.168.0.9
/tmp/test1 192.168.0.0/24
```

http://blog.csdn.net/Until_U

6）启动NFS

```
[root@localhost /]# service rpcbind start
[root@localhost /]# service nfs start
启动 NFS 服务：                                            [确定]
关掉 NFS 配额：                                            [确定]
启动 NFS mountd：                                          [确定]
启动 NFS 守护进程：                                        [确定]
正在启动 RPC idmapd：                                      [确定]
```

显示所有服务的端口

Rpcinfo p

Nfs为2049 portmapper为111

3、 防火墙配置规则

直接编辑防火墙规则

Iptables–I INPUT –s 192.168.0.0/24 –p tcp –m multiport –dports 111,2049,875,892,32803 –jACCEPT

Iptables–I INPUT –s 192.168.0.0/24 –p udp –m multiport –dports 111,2049,875,892,32803 –jACCEPT

下面重启一下防火墙，service Iptables save 然后重启：service Iptables restart

4、 Client-9：

```
23  showmount -e 192.168.0.99
24  mkdir /home/test1 /home/test2
25  mount -t nfs 192.168.0.99:/tmp/nfs-test1 /home/test1
26  mount -t nfs 192.168.0.99:/tmp/nfs-test2 /home/test2
27  ll /home/test1
28  ll /home/test2
29  touch /tmp/nfs-test1/a2
30  touch /home/test1/a2
31  mount -t nfs 192.168.0.99:/tmp/nfs-test1 /home/test1
```

在nfs-test1创建一个a2的文件，在nfs服务器便可以看到

Client -10：

```
50  showmount -e 192.168.0.99
51  mkdir /home/gsq1 /home/gsq2
52  mount -t nfs 192.168.0.99:/tmp/nfs-test1 /home/gsq1
53  mount -t nfs 192.168.0.99:/tmp/nfs-test2 /home/gsq2
```

```
[root@localhost 桌面]# mount -t nfs 192.168.0.99:/tmp/nfs-test2 /home/gsq2
mount.nfs: access denied by server while mounting 192.168.0.99:/tmp/nfs-test2
[root@localhost 桌面]#
```

七、 代理服务器

刚开始还是基础网络搭建，然后在网关上安装squid，并配置

```
[root@lyy ~]# yum install squid -y      //安装squid
[root@lyy ~]# gedit /etc/squid/squid.conf    //进入squid的配置文件
```

修改配置文件如下：

启动squid服务器并初始化缓存目录

[root@lyy ~]# service squid start　　//启动squid服务
[root@lyy ~]# squid -z　　//初始化缓存目录

放行3128端口

```
[root@lyy ~]# iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 3128 -j ACCEPT
```

下面就是在内网中设置代理服务器

打开Firefox浏览器——编辑——首选项——高级——网络——设置——手动配置代理

再次访问外网，在外网中抓包可以看出。或者在网关上停止squid服务器，在内网上再次访问，会收到代理服务器拒绝的信息。

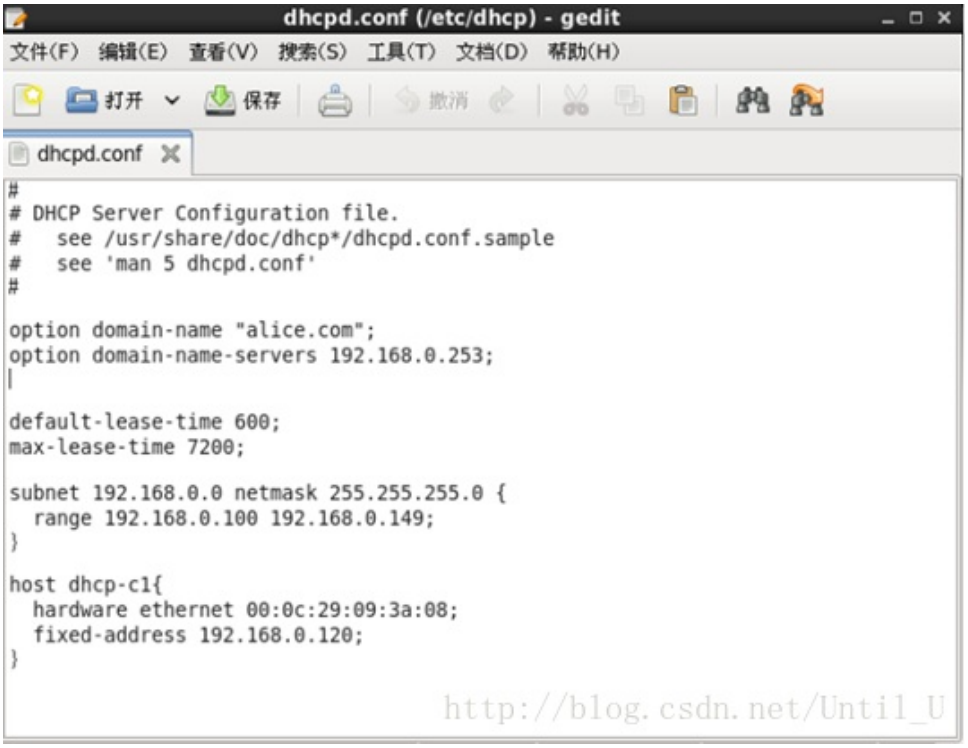
八、DHCP服务器

三台虚拟机：一台做服务器，一台动态随机分配地址，另一台分配固定的IP

基本的配置就不说了，记得给两台客户机ip获取方式设置为DHCP

安装DHCP服务器 yum install dhcp –y

主要配置的文件:

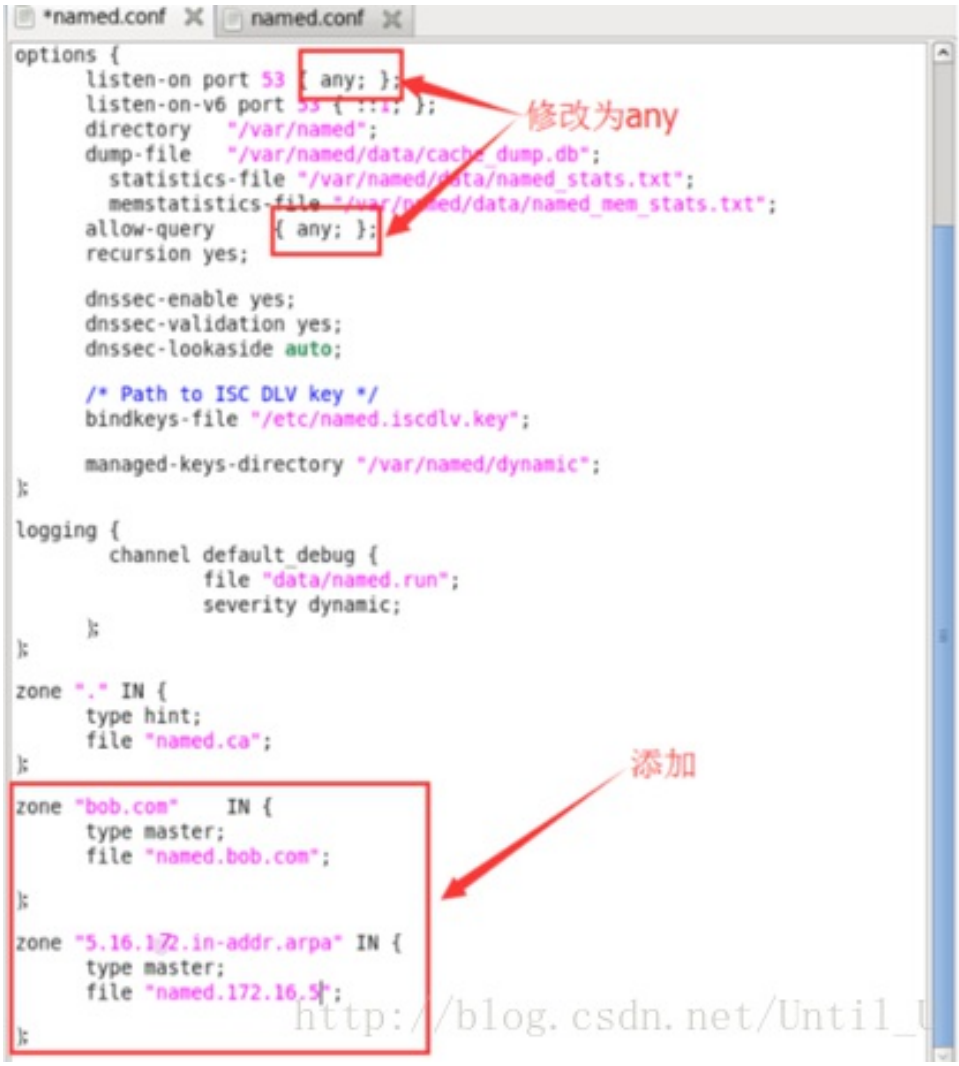


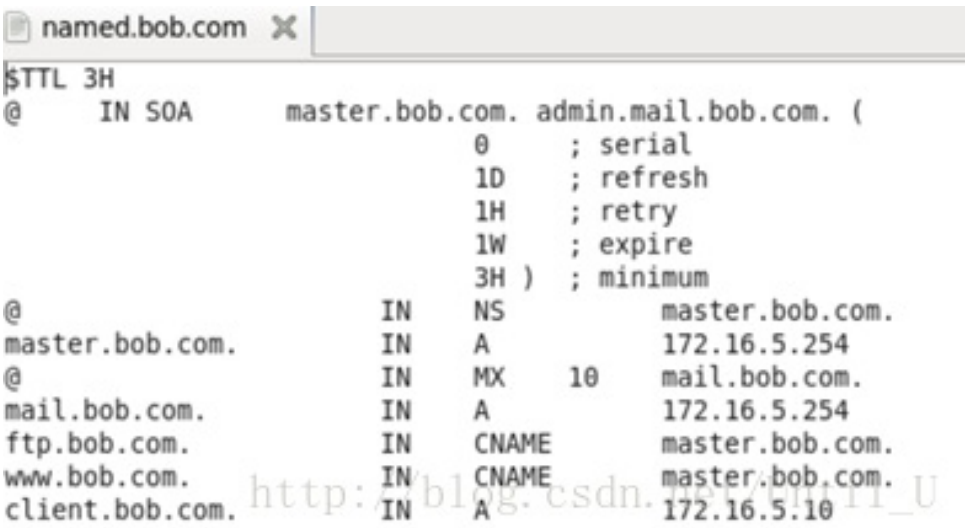
配置完就重启DHCP：service dhcpd restart

下面就可以查看客户机的ip来验证DHCP是否生效！

九、DNS服务器

1. 入门：先安装DNS服务器，再配置主配置文件，正解文件，反解文件，重启named,然后配置防火墙。在客户端设置一下nameserver就ok了。


*named.conf
named.conf
options {
listen-on port 53 { any; };
listen-on-v6 port 53 { ::1; };
directory "/var/named";
dump-file "/var/named/data/cache_dump.db";
statistics-file "/var/named/data/named_stats.txt";
memstatistics-file "/var/named/data/named_mem_stats.txt";
allow-query { any; };
recursion yes;
dnssec-enable yes;
dnssec-validation yes;
dnssec-lookaside auto;
/* Path to ISC DLV key */
bindkeys-file "/etc/named.iscdlv.key";
managed-keys-directory "/var/named/dynamic";
};
logging {
channel default_debug {
file "data/named.run";
severity dynamic;
};
};
zone "." IN {
type hint;
file "named.ca";
};
zone "bob.com" IN {
type master;
file "named.bob.com";
};
zone "5.16.172.in-addr.arpa" IN {
type master;
file "named.172.16.5";
};
修改为any
添加


named.bob.com
$TTL 3H
@ IN SOA master.bob.com. admin.mail.bob.com. (
0 ; serial
1D ; refresh
1H ; retry
1W ; expire
3H) ; minimum
@ IN NS master.bob.com.
master.bob.com. IN A 172.16.5.254
@ IN MX 10 mail.bob.com.
mail.bob.com. IN A 172.16.5.254
ftp.bob.com. IN CNAME master.bob.com.
www.bob.com. IN CNAME master.bob.com.
client.bob.com. IN A 172.16.5.10

named.172.16.5

```
$TTL 3H
@       IN SOA      master.bob.com. admin.mail.bob.com. (
                                    0       ; serial
                                    1D      ; refresh
                                    1H      ; retry
                                    1W      ; expire
                                    3H )    ; minimum
@               IN      NS          master.bob.com.
254             IN      PTR         master.bob.com.
254             IN      PTR         mail.bob.com.
10              IN      PTR         client.bob.com.
```

http://blog.csdn.net/Until_U

```
[root@lyy named]# service named restart
```

```
[root@lyy named]# service named restart
停止 named:                                [确定]
启动 named:                                [确定]
```

7）启动WEB服务

```
[root@lyy named]# service httpd restart
```

8）防火墙设置

开放53端口的tcp以及udp和80端口：

```
[root@lyy named]# iptables -I INPUT -p tcp --dport 53 -j ACCEPT
[root@lyy named]# iptables -I INPUT -p udp --dport 53 -j ACCEPT
[root@lyy named]# iptables -I INPUT -p tcp -m state --state NEW -m tcp  --dport 80 -
j ACCEPT
```

http://blog.csdn.net/Until_U

```
[root@lyy 桌面]# gedit /etc/resolv.conf
```

resolv.conf (/etc) - gedit

文件(F) 编辑(E) 查看(V) 搜索(S) 工具(T) 文档(D) 帮助(H)

打开 保存 撤消

resolv.conf

```
# Generated by NetworkManager


# No nameservers found; try putting DNS servers into your
# ifcfg files in /etc/sysconfig/network-scripts like so:
#
# DNS1=xxx.xxx.xxx.xxx
# DNS2=xxx.xxx.xxx.xxx
# DOMAIN=lab.foo.com bar.foo.com
nameserver 172.16.5.254
```

http://blog.csdn.net/Until_U

主从DNS服务器：

主DNS：

named.conf

```
options {
        listen-on port 53 { any; };
        directory   "/var/named";
        dump-file   "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
        allow-transfer {192.168.0.253; };
};


zone "." IN {
        type hint;
        file "named.ca";
};

zone "alice.com"  IN {
        type master;
        file "named.alice.com";

};

zone "0.168.192.in-addr.arpa" IN {
        type master;
        file "named.192.168.0";
};
```

http://blog.csdn.net/Until_U

named.alice.com

```
$TTL 3H
@       IN SOA      master.alice.com. admin.mail.alice.com. (
                                0       ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum
@                       IN      NS              master.alice.com.
master.alice.com.       IN      A               192.168.0.254
@                       IN      NS              slave.alice.com.

slave.alice.com.        IN      A               192.168.0.253
@                       IN      MX      10      mail.alice.com.

mail.alice.com.         IN      A               192.168.0.254
ftp.alice.com.          IN      CNAME           master.alice.com.
www.alice.com.          IN      CNAME           master.alice.com.
client.alice.com.       IN      A               192.168.0.10
```

http://blog.csdn.net/Until_U

named.192.168.0

```
$TTL 3H
@       IN SOA      master.alice.com. admin.mail.alice.com. (
                                0       ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum
@           IN      NS          master.alice.com.

@           IN      NS          slave.alice.com.

254         IN      PTR         master.alice.com.

253         IN      PTR         slave.alice.com.

254         IN      PTR         mail.alice.com.
10          IN      PTR         client.alice.com.
```

http://blog.csdn.net/Until_U

辅助DNS：只需配置主配置文件！

named.conf

```
options {
      listen-on port 53 { any; };
      directory   "/var/named";
      dump-file   "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";

};

zone "alice.com" IN {
      type slave;
      file "slaves/named.alice.com";
      masters {192.168.0.254;};
};

zone "0.168.192.in-addr.arpa" IN {
      type slave;
      file "slaves/named.192.168.0";
      masters {192.168.0.254;};
};
```

http://blog.csdn.net/Until_U

多域：不想写了！大概截个图：

```
options {
    listen-on port 53 { any; };
    directory     "/var/named";
    dump-file     "/var/named/data/cache_dump.db";
      statistics-file "/var/named/data/named_stats.txt";
      memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query     { any; };
    allow-transfer {none; };
};

zone "." IN {
    type hint;
    file "named.ca";
};

zone "com"    IN {
    type master;
    file "named.com";
};
```

http://blog.csdn.net/Until_U

named.com

```
$TTL 3H
@       IN SOA      master.com. admin.mail.com. (
                                0       ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum
@                       IN      NS          master.com.
master.com.             IN      A           192.168.0.254
alice.com.              IN      NS          master.alice.com.
master.alice.com.       IN      A           192.168.0.253
bob.com.                IN      NS          master.bob.com.
master.bob.com.         IN      A           202.3.4.253
```

http://blog.csdn.net/Until_U

其他两台参照前面就行了。

十、邮件服务器

在多域的基础上操作：

```
[root@lyy 桌面]# gedit /etc/postfix/main.cf
```

http://blog.csdn.net/Until_U

```
home_mailbox = Maildir/
html_directory = no
inet_interfaces = all
inet_protocols = ipv4
mail_owner = postfix
mailq_path = /usr/bin/mailq.postfix
manpage_directory = /usr/share/man
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
mydomain = alice.com
myhostname = mail.alice.com
mynetworks = 127.0.0.0/8
myorigin = $mydomain
newaliases_path = /usr/bin/newaliases.postfix
queue_directory = /var/spool/postfix
readme_directory = /usr/share/doc/postfix-2.6.6/README_FILES
relay_domains = $mydestination, bob.com
sample_directory = /usr/share/doc/postfix-2.6.6/samples
sendmail_path = /usr/sbin/sendmail.postfix
setgid_group = postdrop
smtpd_client_restrictions = permit_sasl_authenticated
smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated,
reject_unauth_destination
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain = $myhostname
smtpd_sasl_security_options = noanonymous
unknown_local_recipient_reject_code = 550
```

http://blog.csdn.net/Until_U

获得sasl的认证

- 将/etc/sysconfig/saslauthd文件中的MECH=pam改为 MECH=shadow

http://blog.csdn.net/Until_U

- 启动saslauthd

```
[root@lyy 桌面]# service saslauthd start
```

- 解除SELinux的限制（需要等待20s左右）

```
[root@lyy 桌面]# setsebool -P allow_saslauthd_read_shadow 1
```

- 验证是否能够使用系统上的账号密码来进行认证

```
[root@lyy 桌面]# testsaslauthd -u user1 -p 123456 (你的密码)
```

```
[root@lyy 桌面]# testsaslauthd -u user1 -p 123456
0: OK "Success."
```

7）安装dovecot服务

```
[root@lyy 桌面]# yum install dovecot -y
```

8）配置dovecot服务（需要修改4个文件）

```
[root@lyy 桌面]# gedit /etc/dovecot/dovecot.conf
```

http://blog.csdn.net/Until_U

dovecot文件编辑看书

下面网关上的防火墙规则：

```
[root@localhost 桌面]# iptables-save
# Generated by iptables-save v1.4.7 on Wed Dec 13 16:11:20 2017
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -p icmp -j ACCEPT
-A FORWARD -p tcp -m multiport --dports 25,110 -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Wed Dec 13 16:11:20 2017
```

http://blog.csdn.net/Until_U

另外的两台DNS服务器也要配置防火墙规则：只要在INPUT链中放行53、25、110端口就ok了。

最后就是两个客户端注册邮件用户，先安装thunderbird，再注册，最后发邮件。

还有就是Web和ftp服务器，都挺简单的，而且书上都有相关的操作。也可以参考我另一篇文章哦

链接：Linux实验（邮件服务器、web服务器和vsftp服务器）