Vipul Sharma B17069
Swapnil Rustagi B17104

CS307
System Practicum
Assignment 3
Report

Youtube Video Demo Link -
https://www.youtube.com/watch?v=qSqgTdcWdh4

1. **Creating VMs**

a. Web Server

Install apache2

```
sudo apt install apache2
```

Allow traffic from port 80

```
sudo ufw allow in "Apache"
```

Get your internet interface used from

```
ip a
```

Output for me was -

```
vipul@vipul-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state
UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:0b:3a:bc brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.8/24 brd 192.168.1.255 scope global dynamic
enp0s3
       valid_lft 86337sec preferred_lft 86337sec
    inet6 fe80::c597:174b:5181:7f2/64 scope link
       valid_lft forever preferred_lft forever
```

So use enp0s3 for getting IP Address.

The corresponding IP Address is -
192.168.1.8

Open this IP Address on your VM to verify if apache is working correctly. Same page

should open up on the localhost of your VM as well.

Install MySQL-
```
sudo apt install mysql-server
```

Run script after installation -
```
sudo mysql_secure_installation
```

Test installation using -
```
sudo mysql
```

Install PHP-
```
sudo apt install php libapache2-mod-php php-mysql
```

Test installation version using -
```
php -v
```

cd /var/www
sudo mkdir swapnil
sudo mkdir vipul
sudo chown -R $USER:$USER /var/www/vipul
sudo chown -R $USER:$USER /var/www/swapnil

1. Create index.html files with random text in both these directories.

2. Do “sudo nano /etc/apache2/sites-available/vipul.conf” and put the following contents.

```
<VirtualHost *:80>
      ServerName vipul.firewall.net
      ServerAdmin webmaster@localhost
      DocumentRoot /var/www/vipul
      ErrorLog ${APACHE_LOG_DIR}/error.log
      CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

3. Do “sudo nano /etc/apache2/sites-available/swapnil.conf” and put the following contents. Repeat for vipul.

```
 <VirtualHost *:80>
      ServerName swapnil.firewall.net
      ServerAdmin webmaster@localhost
      DocumentRoot /var/www/swapnil
      ErrorLog ${APACHE_LOG_DIR}/error.log
```

```
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

4. sudo a2ensite vipul.conf
5. sudo a2ensite swapnil.conf
6. sudo service apache2 reload

b. SMTP Server

1. `sudo DEBIAN_PRIORITY=low apt-get install postfix`
This installs mail server postfix, while prompting for configuration:

Configuration filled:

General type of mail configuration?: Internet Site
System mail name: firewall.net
Root and postmaster mail recipient: swapnil
Other destinations to accept mail for (blank for none): (default value)
Force synchronous updates on mail queue?: No
Local networks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 (default value)
Mailbox size limit: 0 (no limit)
Local address extension character: + (default value)
Internet Protocols: all

2. sudo postconf -e 'home_mailbox= Maildir/'
3. sudo postconf -e 'virtual_alias_maps= hash:/etc/postfix/virtual'
4. sudo nano /etc/postfix/virtual

Put the following into the file and save:

```
node1@firewall.net swapnil@10.0.0.1
node2@firewall.net swapnil@10.0.0.2
admin@firewall.net swapnil
```

5. Follow steps 4,5,6 and 7 as it is from
https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-postfix-on-ubuntu-16-04

c. DNS Server

1. `sudo apt install bind9`
2. `sudo nano /etc/bind/named.conf.local`

Append this to the end of the file and save:

```
zone "firewall.net" {
      type master;
      file "/etc/bind/db.firewall.net";
};
```

3. sudo cp /etc/bind/db.local /etc/bind/db.firewall.net
4. Edit /etc/bind/db.firewall.net to have following contents

```
;
; BIND data file for firewall.net
;
$TTL  604800
@     IN    SOA   firewall.net. root.firewall.net. (
                              7          ; Serial
                         604800      ; Refresh
                         86400       ; Retry
                         2419200          ; Expire
                         604800 )    ; Negative Cache TTL
;
@     IN    NS    ns
@     IN    MX    10 mail
@     IN    A     10.1.0.1
ns    IN    A     10.1.0.1
mail  IN    A     10.1.0.2
swapnil IN        A     10.1.0.1
vipul   IN        A     10.1.0.1
```

5. `sudo nano /etc/bind/named.conf.options`

Edit the file so that it looks like this:

```
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.
```

```
    forwarders {
         8.8.8.8;
    };

    allow-query { any; };
    allow-recursion { any; };
    forward only;



//========================================================================
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See
https://www.isc.org/bind-keys

//========================================================================
    dnssec-validation auto;

    auth-nxdomain no;  # conform to RFC1035
    listen-on-v6 { any; };
};
```

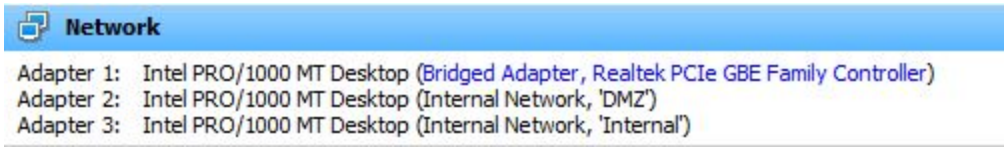
6. sudo systemctl restart bind9.service

d. VMs for machines in internal zone

1. In the internal network VMs (10.0.x.x), in IPv4 configuration, put DNS as 10.1.0.3.

e. VM for gateway/firewall machine

Create VM with following network config -



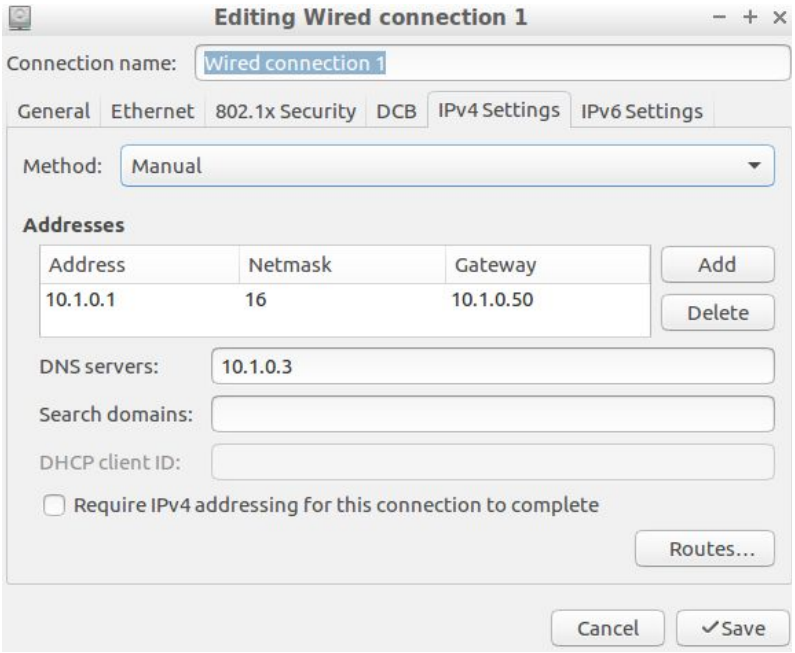
Adapter1 : enp0s3 : 192.168.1.5
Adapter2 : enp0s8 : 10.1.0.50
Adapter3: enp0s9 : 10.0.0.50

2. **Creating Different Networks**

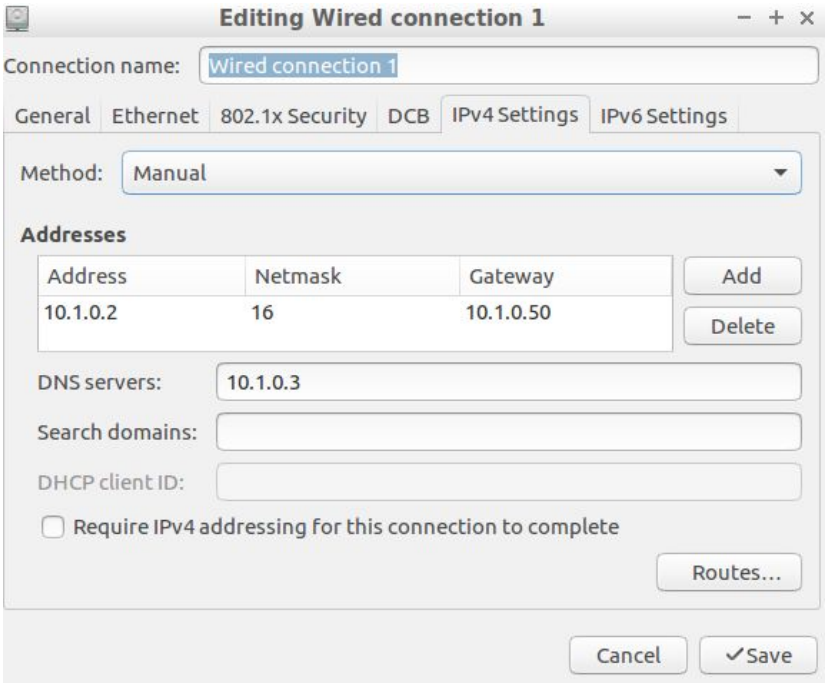
Attach WebServer, DNS, SMTP to adapter for Internal Network ‘DMZ’.

Attach Node1,Node2,Node3 to adapter for Internal Network ‘Internal’.
Attach Gateway to adapters for Internal Networks ‘DMZ’ and ‘Internal’ and also to bridge networks to gain internet access.

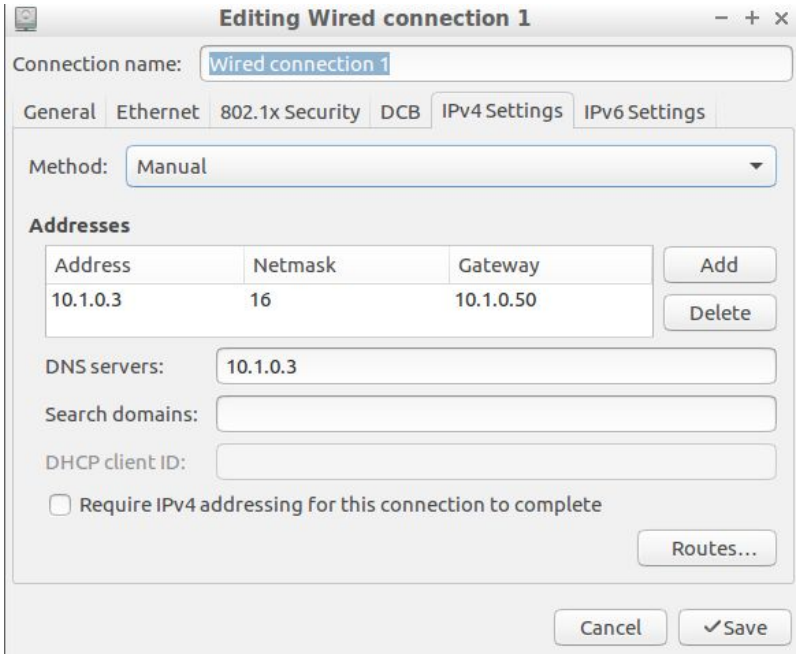
Configure nodes with their config -
1. Web Server



2. SMTP



3. DNS



3. **Configuring gateway/firewall**

Open superuser terminal using sudo su to execute all below commands.

a.
In gateway machine -
echo 1 > /proc/sys/net/ipv4/ip_forward

b.
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

c.

Here,
enp0s3 = network adapter connected to Internet
enp0s9 = network adapter connected to Internal network
enp0s8 = network adapter connected to DMZ

iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
iptables -A FORWARD -i enp0s3 -o enp0s9 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s3 -j ACCEPT

Test using
ping 216.58.221.46
// ping to google from internal node using ip (assuming dns is not working yet)

d.
iptables -N dmznet
iptables -A dmznet -i enp0s3 -o enp0s8 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A dmznet -i enp0s8 -o enp0s3 -j ACCEPT

To enable -
iptables -A FORWARD -j dmznet

To delete -
iptables -D FORWARD -j dmznet

After enabling install open ssh server on all DMZ servers-

sudo nano /etc/resolv.conf
// Add line ‘nameserver 8.8.8.8’ to the above file.
// Might also need to remove the dns server from the connection settings which we configured earlier.
sudo apt install openssh-server
sudo systemctl status ssh
sudo systemctl enable ssh
sudo ufw allow ssh
sudo ufw enable
sudo ufw status

e.
iptables -A PREROUTING -t nat -i enp0s3 -p tcp --dport 80 -j DNAT --to 10.1.0.1:80
iptables -A FORWARD -p tcp -d 10.1.0.1 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.1.0.1 --sport 80 -j ACCEPT

iptables -A PREROUTING -t nat -i enp0s3 -p tcp --dport 443 -j DNAT --to 10.1.0.1:443
iptables -A FORWARD -p tcp -d 10.1.0.1 --dport 443 -j ACCEPT
iptables -A FORWARD -p tcp -s 10.1.0.1 --sport 443 -j ACCEPT

iptables -A PREROUTING -t nat -i enp0s3 -p tcp --dport 25 -j DNAT --to 10.1.0.2:25
iptables -A FORWARD -p tcp -d 10.1.0.2 --dport 25 -j ACCEPT

iptables -A FORWARD -p tcp -s 10.1.0.2 --sport 25 -j ACCEPT

iptables -A PREROUTING -t nat -i enp0s3 -p udp --dport 53 -j DNAT --to 10.1.0.3:53
iptables -A FORWARD -p udp -d 10.1.0.3 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -s 10.1.0.3 --sport 53 -j ACCEPT

f.
iptables -A FORWARD -i enp0s9 -o enp0s8 -p tcp --dport 22 -s 10.0.0.1 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -p tcp --sport 22 -d 10.0.0.1 -m state --state ESTABLISHED -j ACCEPT