

# Systems Practicum (CS307)

## Assignment 3

### Group 1

#### Members:

- Ravi Kumar (B19191)
- Prashant Kumar (B19101)
- Gaurav Sahitya (B19083)
- Shubham Saurav (B19222)
- Sagar Tarafdar (B19110)
- Saloni Patidar (B19111)

#### 1.

##### A. Creating the Web-Server

1. Installing Apache2 on the Web-Server machine

```
sudo apt install apache2
```

2. Running the apache2 service

```
sudo service apache2 start
```

3. Adding the hosts

- a. In the `/etc/hosts` file add the following

```
127.0.0.1 ravi.firewall.net
127.0.0.1 prashant.firewall.net
127.0.0.1 saloni.firewall.net
127.0.0.1 sagar.firewall.net
127.0.0.1 gaurav.firewall.net
127.0.0.1 shubham.firewall.net
```

- b. In the `/var/www` directory create folders with names mentioned above

- c. In the `/etc/apache2/site-available` create configuration files with the name as `<member-name>.conf` and add following content to it

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

4. Then run the following commands to enable the sites

```
a2ensite prashant.conf
a2ensite <member-name.conf>
```

5. To allow access from the outside, allow the incoming connections for apache in the firewall,

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

6. Restart the Apache service,

```
sudo service apache2 restart
```

## B. Creating the SMTP Server

1. Changing the hostname to the mail server  
`sudo hostnamectl set-hostname mail.firewall.net`
2. Installing postfix,  
`sudo DEBIAN_PRIORITY=low apt install postfix`
3. Configuring postfix for our use,  
`sudo dpkg-reconfigure postfix`
  - a. General Type of mail configuration?: Internet Site
  - b. System mail name: firewall.net
  - c. Root and postmaster mail recipient: smtp
  - d. Other Destinations to accept mail from: firewall.net, localhost.localdomain, localhost
  - e. Force Synchronous updates on mail queue?: No
  - f. Local Networks: 127.0.0.0/8  
[::ffff:127.0.0.0]/104[::1]/128
  - g. Mailbox size limit: 0 (No Limit)
  - h. Local Address extension character: +
  - i. Internet Protocols to use: all
4. `sudo postconf -e 'home_mailbox=Maildir/'`  
`sudo postconf -e 'virtual_alias_maps=hash:/etc/postfix/virtual'`
5. In the file `'/etc/postfix/virtual'` add the following,  
[contact@firewall.net](mailto:contact@firewall.net) smtp  
[admin@firewall.net](mailto:admin@firewall.net) smtp
6. `echo 'export MAIL=~/.Maildir' | sudo tee -a /etc/bash.bashrc`  
`| sudo tee -a /etc/profile.d/mail.sh`  
`source /etc/profile.d/mail.sh`
7. Installing the mailing client,  
`sudo apt install s-nail mailutils`
8. Configuring s-nail,  
`sudo nano /etc/s-nail.rc`  
At the end of this file add the following,  
`set emptystart`  
`set folder=Maildir`  
`set record=+sent`
9. Altering the Firewall Rules,  
`sudo ufw allow 25/tcp`  
`sudo ufw allow Postfix`  
`sudo ufw enable`

### C. Creating the DNS Server

1. Installing Bind services,

```
sudo apt-get install bind9
```

2. In the file `/etc/bind/named.conf.local` add,

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

3. In the file `/etc/bind/named.conf` make sure these lines are present,

```
include "/etc/bind/named.conf.options";  
include "/etc/bind/named.conf.local";  
include "/etc/bind/named.conf.default-zones";
```

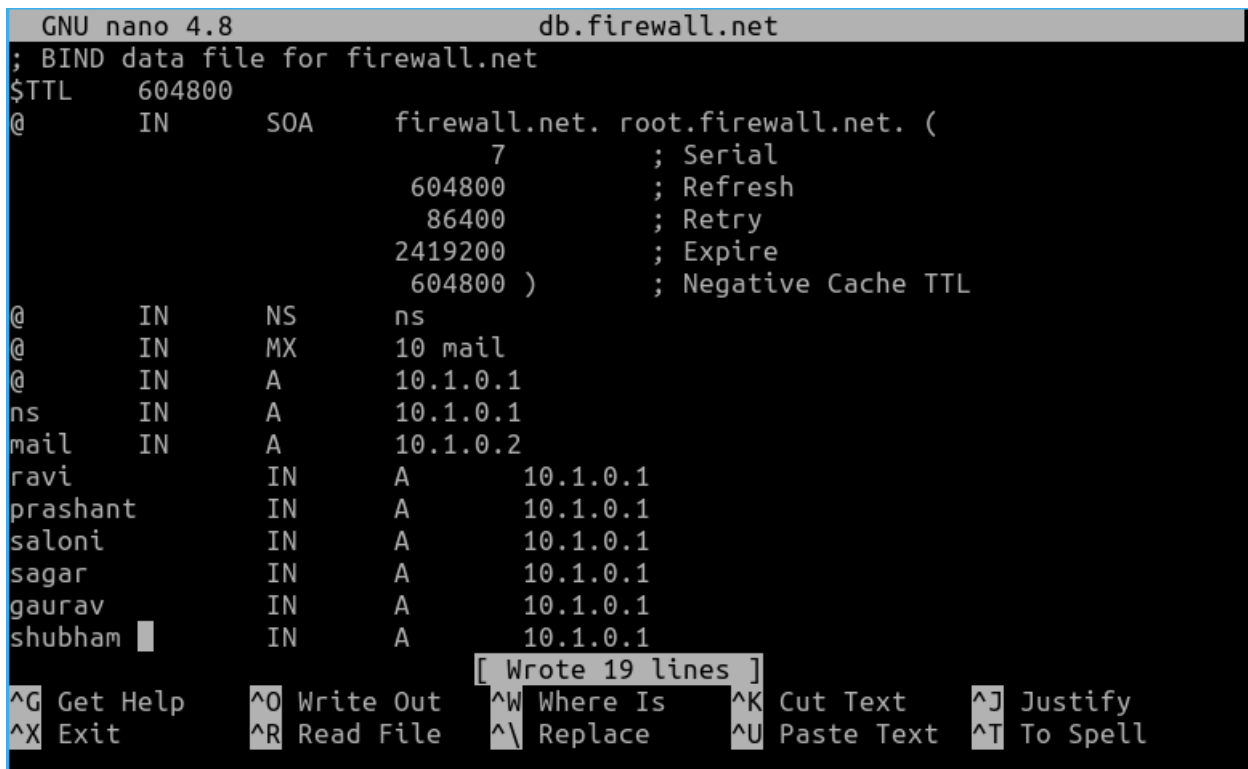
4. In the file `/etc/bind/named.conf.options` add the following,

```
forwarders {  
    8.8.8.8;  
};  
allow-query { any; };  
allow-recursion { any; };  
forward only;
```

```
dnssec-validation auto;
```

```
listen-on-v6 { any; };
```

5. Create a file name `"db.firewall.net"` and write this,



```
GNU nano 4.8 db.firewall.net  
; 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  
ravi      IN      A        10.1.0.1  
prashant  IN      A        10.1.0.1  
saloni    IN      A        10.1.0.1  
sagar     IN      A        10.1.0.1  
gaurav    IN      A        10.1.0.1  
shubham   IN      A        10.1.0.1  
[ Wrote 19 lines ]  
^G Get Help      ^O Write Out     ^W Where Is      ^K Cut Text      ^J Justify  
^X Exit          ^R Read File     ^_ Replace       ^U Paste Text    ^T To Spell
```

6. Restart the bind service,  
*sudo systemctl restart bind9.service*

## 2. Creating Virtual Machines

### A. The Gateway Machine

In the Gateway Machine we have three adapters,

1. enp0s3 - Interface to the Internet
2. enp0s8 - Interface to the 'DMZ' zone (10.1.0.4)
3. enp0s9 - Interface to the 'Internal' Network (10.0.0.4)

### B. Web-Server

It only has one Interface which is connected to the gateway machine

enp0s3 - 10.1.0.1

DNS - 10.1.0.3

Gateway - 10.1.0.4

### C. SMTP Server

It only has one Interface which is connected to the gateway machine

enp0s3 - 10.1.0.2

DNS - 10.1.0.3

Gateway - 10.1.0.4

### D. DNS Server

It only has one Interface which is connected to the gateway machine

enp0s3 - 10.1.0.3

DNS - 10.1.0.3

Gateway - 10.1.0.4

### E. Node1

It only has one Interface which is connected to the gateway machine

enp0s3 - 10.0.0.1

DNS - 10.1.0.3

Gateway - 10.0.0.4

## Configuring the Iptable Rules

1.

*iptables -P INPUT DROP*

*iptables -P FORWARD DROP*

*iptables -P OUTPUT ACCEPT*

2.

*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*

3. Creating a New Table

*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
iptables -A FORWARD -j dmznet To delete - iptables -D FORWARD -j dmznet
```

#### 4. Enabling Services from the Web-Server

```
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
```

#### 5. Enabling services for the mail server

```
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
```

#### 6. Enabling services from the DNS Server

```
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
```

#### 7. Enabling SSH from 10.0.0.1 to DMZ

```
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
```