

**Indian Institute of Technology Mandi**  
**Feb - June 2022**  
**CS307 - System Practicum**  
**Assignment 3**  
**Course Instructor: Aditya Nigam**  
**Date : 10 April 2022**

**Instructions:**

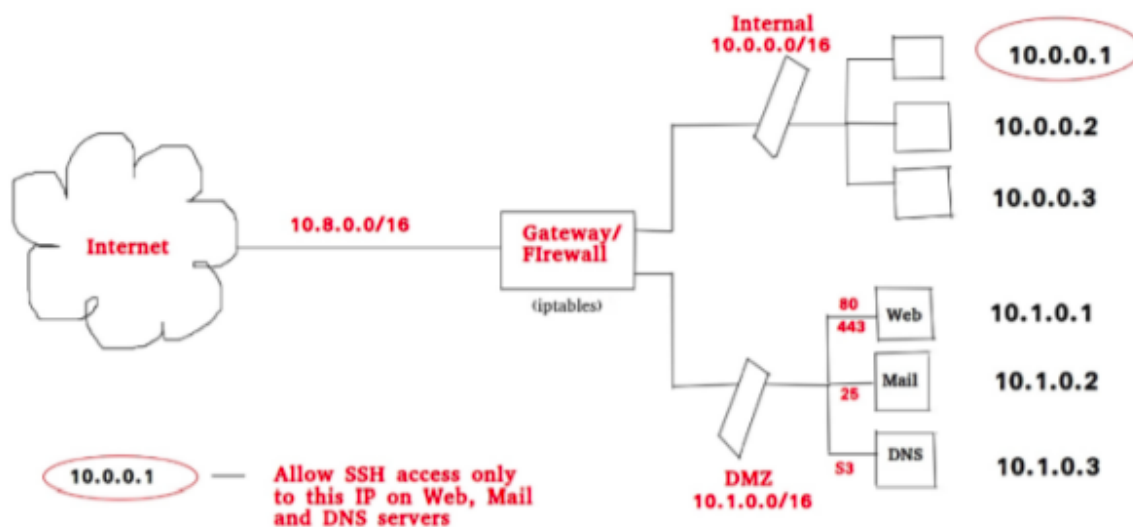
- Plagiarism is strictly prohibited. In case of violation, a zero will be awarded for this assignment as a warning and a quick F grade if repeated later.
- Contact Adarsh (b18100@students.iitmandi.ac.in) or Arshita (b18105@students.iitmandi.ac.in) for any queries.
- Prefer using namespaces over VMs if your PC has RAM less than 8 GB.
- Use ubuntu in case you are using VMs for less RAM usage

**Server Configuration:**

A system administrator, or sysadmin, is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers.

In this assignment you will explore such tasks, through VMs or namespaces or docker containers.

We use web servers, mail servers, Domain Name Servers everyday. Through this assignment, we will learn how to configure them. Further, we will learn how to place them in a demilitarized zone and allow protected access using iptables. We will also learn about concepts such as Network Address Translation (NAT), and port-forwarding. Figure below shows the expected outcome of this assignment.



The firewall isolates the external Internet from the Intranet. The Intranet is subdivided into two zones, the internal zone and the demilitarized zone. Of the two, the internal zone is a more protected environment with no access from the external world (Internet hosts). The demilitarized zone allows access from the external world to some degree to services running on specific ports. For example, the ports 80 and 443 corresponding to http and https are open on the web server, and nothing else. The demilitarized zone hosts the web server, SMTP server and a DNS server that can be accessed from external as well as internal zones. Additionally, a specific host on the internal zone 10.0.0.1 must be allowed ssh access on port 22 to the web, mail and DNS servers. The servers in the demilitarized zone normally do not have access to the Internet but during upgrades access to the Internet should be temporarily enabled. The machines in the Internal zone should be given access to the Internet.

For this lab, we will create different VMs/namespaces corresponding to the hosts shown in Figure. The different tasks in this assignment are listed below:

### 1. Creating VMs/ namespaces:

You need to use one from VMs and namespaces. VMs will require more RAM. If you are low on RAM, prefer using namespaces. Refer to tutorials in references for both. Create the following VMs/namespaces:

- a. Web server (apache 2 server with a subdomain corresponding to your course group member names. e.g. teammember1.firewall.net , teammember2.firewall.net and host your personal pages on these domains).
- b. SMTP server

- c. DNS server
- d. VMs/ namespaces to simulate internal zones.
- e. If you are using namespaces, you can use your machine as the firewall/gateway. Use [firejail](#) to sandbox any process in a network namespace. If you are using VMs, you need to create a separate VM for firewall/gateway
- f. If you want to reduce the number of VMs, you can have Web Server and SMTP on the same VM.

## **2. Create the different networks as shown in the figure.**

Refer to <https://www.virtualbox.org/manual/ch06.html> for the different networking modes available in Virtual box. In case you are using namespaces, refer to <https://medium.com/@abhishek.amjeet/container-networking-using-namespaces-part1-859d317ca1b8#:~:text=The%20Linux%20kernel%20provides%20own%20filesystem%20using%20mnt%20namespace>

## **3. Configuring the gateway/firewall VM or namespace:**

- (a) As a router to forward packets.
- (b) Setup default firewall policies using iptables to drop all incoming and forwarding packets and accept only outgoing packets. Refer to manual pages for iptables or <https://en.wikipedia.org/wiki/Iptables>
- (c) Enable the internal zone to access the Internet using iptables. Here we use Network Address Translation. As the machines in the internal zone belong to a private network, their packets need to be forwarded by the gateway. This can be done by enabling NAT for the packets arriving from this network. In other words, these packets arriving at the gateway have their source address belonging to the internal network.
- (d) Create a custom chain to enable the DMZ to access the Internet using iptables – N dmznet. Later disable it by deleting the rule from iptables.
- (e) Enable access to the DMZ on specific ports for the external network: Here, we use the concept of port forwarding. As the DMZ is a private network, it cannot be accessed from outside. To enable access, we map certain ports on the firewall to machines on the DMZ. Thus, whenever packets arrive at the firewall destined to those ports, they are forwarded to the mapped hosts on the DMZ.
- (f) Enable ssh access only from 10.0.0.1 to DMZ hosts.

**4. Test whether the above configuration works correctly:** by opening/pinging web pages from internal/external networks, sending emails etc.

You might face issues while networking the namespaces in case you are behind the institute proxy. Try disabling that if you face issues. Also refer to point 2 in namespaces under references in case you are facing any issue with firejail.

### **Note:**

In case someone is comfortable using docker containers for the above task, he/she is free to use containers instead of namespaces/VMs.

**References for Help Namespaces :**

1. <https://l3net.wordpress.com/2014/06/08/securing-a-web-server-using-a-linux-namespaces-sandbox/>
2. <https://github.com/netblue30/firejail/issues/3184#issuecomment-579300756>

**VMs :**

1. <https://www.virtualbox.org/>
2. <https://www.virtualbox.org/manual/ch06.html>

**IPTables :**

1. <https://en.wikipedia.org/wiki/Iptables>
2. <https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html>
3. <http://sweet.ua.pt/andre.zuquete/Aulas/SAR/13-14/docs/g2-iptables.pdf>

**Mail Server :**

<https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-postfix-on-ubuntu-16-04>

**DNS Server :**

<https://osttechnix.com/install-and-configure-dns-server-ubuntu-16-04-lts/>

**Useful Video Tutorials :**

1. Web Server: <https://www.youtube.com/watch?v=Nu-18s6EeM8>
2. Mailserver: <https://www.youtube.com/watch?v=x28ciavQ4mI>
3. DNS: <https://www.youtube.com/watch?v=T-eghY-9WdE> and <https://www.youtube.com/watch?v=mpQZVYPuDGU>
4. Firewall: [https://www.youtube.com/watch?v=XEqnE\\_sDzSk](https://www.youtube.com/watch?v=XEqnE_sDzSk)