IPTables: Port Forwarding - Lab Guide

This lab was developed by Sparta Global for Cybersecurity courses. It was built based on the original lab that was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under National Science Foundation Award No. 1438893. This work is in the public domain, and cannot be copyrighted.

1 Overview

Iptables is a command line software-based firewall in Linux. It uses policy chains to allow and to block traffic.

IPTables is used as a Firewall and can perform NAT and PAT operations.

In this lab, we focus on IPTables configuration to allow and deny access from/to IP addresses and/or services.

2 Lab Environment

This lab runs in the Labtainer framework, available at http://my.nps.edu/web/c3o/labtainers. That site includes links to a pre-built virtual machine that has Labtainers installed, however Labtainers can be run on any Linux host that supports Docker containers.

From your labtainer-student (/labtainer/labtainer-student) directory start the lab using:

```
labtainer sparta-port-forwarding
```

A link to this lab guide will be displayed.

3 Network Configuration

IP addresses and routing are configured on all devices.

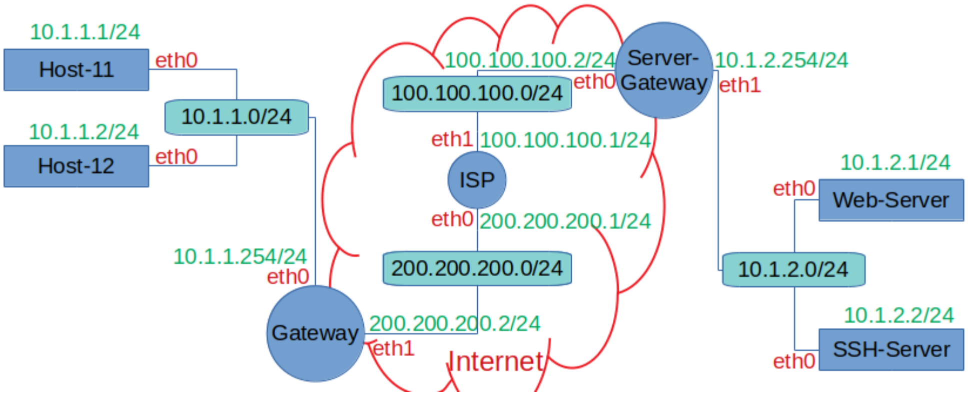

Figure 1: Network topology for routing-basics lab

4 Credentials

- **Host-11**:
  - **Username:** user-11
  - **Password:** user-11
- **Host-12**:
  - **Username:** user-12
  - **Password:** user-12
- **Gateway**:
  - **Username:** admin
  - **Password:** admin
- **ISP**:
  - **Username:** admin
  - **Password:** admin
- **Web-Server**:
  - **Username:** web-admin
  - **Password:** web-admin
- **SSH-Server**:
  - **Username:** ssh-admin
  - **Password:** ssh-admin
- **Server-Gateway**:
  - **Username:** admin
  - **Password:** admin

5 Lab Tasks

5.1 Configuring the NAT Rules on the Gateway

- The default rules in iptables allow all type of traffic to pass.
  - We will start by deleting (flushing) all rules.

    ```
    sudo iptables -F
    sudo iptables -t nat -F
    sudo iptables -X
    ```

  - Drop all packets by default

```
sudo iptables -P FORWARD DROP
sudo iptables -P INPUT   DROP
sudo iptables -P OUTPUT  DROP
```

- Lets run this command that will perform NAT on all packets passing by the gateway and leaving the router from the interface eth0 which is the interface connected to the ISP router in our design and it has the public IP address which is the routable address in the network.

  ```
  sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
  ```

5.2 Configuring the NAT Rules on the Server-Gateway

- The default rules in iptables allow all type of traffic to pass.
  - We will start by deleting (flushing) all rules.

    ```
    sudo iptables -F
    sudo iptables -t nat -F
    sudo iptables -X
    ```

  - Drop all packets by default

    ```
    sudo iptables -P FORWARD DROP
    sudo iptables -P INPUT   DROP
    sudo iptables -P OUTPUT  DROP
    ```

- Now, let configure the Server-Gateway to forward traffic received on its IP address to the servers (TCP80 to Web-Server and TCP22 to SSH-Server). We will start by deleting (flushing) all rules.

  ```
  sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT \
  --to-destination 10.1.2.1:80
  sudo iptables -t nat -A PREROUTING -p tcp --dport 22 -j DNAT  \
  --to-destination 10.1.2.2:22
  sudo iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
  ```

6 Testing the connectivity

- On Host-11 (Send HTTP request Host-11 -> Web-Server to get a web page)

  ```
   wget http://100.100.100.2
  ```

  What is the result ? Which device is sending the response in this case ?

- On Host-11 (SSH Host-11 -> Web-Server)

  ```
  ssh ssh-admin@100.100.100.2
  ```

  What is the result ? Which device is sending the response in this case ?

- On Host-11 (Ping Host-11 -> Web-Server)

```
ping 100.100.100.2
```

What is the result ? Which device is sending the response in this case ?

- On Host-12 (Send HTTP request Host-12 -> Web-Server to get a web page)

  ```
  wget http://100.100.100.2
  ```

  What is the result ? Which device is sending the response in this case ?

- On Host-12 (SSH Host-12 -> Web-Server)

  ```
  ssh ssh-admin@100.100.100.2
  ```

  What is the result ? Which device is sending the response in this case ?

- On Host-12 (Ping Host-12 -> Web-Server)

  ```
  ping 100.100.100.2
  ```

  What is the result ? Which device is sending the response in this case ?

7 Submission

After finishing the lab, go to the terminal on your Linux system that was used to start the lab and type:

```
stoplab sparta-port-forwarding
```

When you stop the lab, the system will display a path to the zipped lab results on your Linux system. Provide that file to your instructor, e.g., via the Sakai site.