IPTables: NAT Rules - Lab Guide

V1.0.1 - Reviewed on 15/08/2021

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-pat
```

A link to this lab guide will be displayed.

3 Network Configuration

IP addresses and routing are configured on all devices.

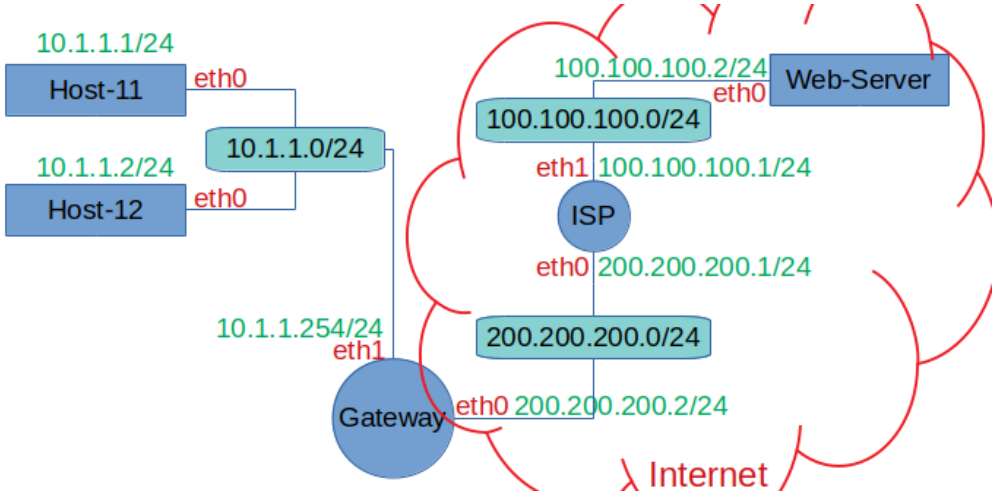

Figure 1: Network topology for routing-basics lab

4 Credentials

- **Host-11**:
  - **Username:** user-11
  - **Password:** user-11
- **Host-12**:
  - **Username:** user-12
  - **Password:** user-12

  o
- **Web-Server**:
  - **Username:** web-admin
  - **Password:** web-admin
- **Firewall**:
  - **Username:** admin
  - **Password:** admin

5 Lab Tasks

5.1 Testing the Initial Configuration

Lets check what we can/can't do in this network.

- On Host-11 (Ping Host-11 -> Gateway: Internal Interface)

```
ping 10.1.1.254
```

What is the result ?

- On Host-11 (Ping Host-11 -> Gateway: External Interface)

  ```
  ping 200.200.200.2
  ```

  What is the result ?

- On Host-11 (Ping Host-11 -> ISP: eth0)

  ```
  ping 200.200.200.1
  ```

  What is the result ?

5.2 Capturing the Traffic

Lets use **tcpdump** which is a command line tool that can capture TCP/IP and other packets being transmitted or received over a network interface.

In the ISP terminal, run the following command:

```
sudo tcpdump -i eth0 -n
```

eth0 is the interface connected to our gateway. You can make sure of that by running **ifconfig** or **ip add**

Now, you can see that the packets are arriving at the ISP router (with their private IP address), but then the ISP router has no routes for private IP addresses that they exist in customers networks so it doesn't know where to send the response.

5.3 Testing the Initial Configuration

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

  ```
  wget http://10.1.2.1/index.html
  ```

  What is the result ?

- Check the router terminal, scroll up to check all the packets captured by the router. Notice that you can find the content of the html page.

  That means the traffic isn't encrypted and the packets (info) can be read by any device on the route between the client and the server.

5.4 Configuring the NAT Rules on the Gateway

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
```

Now, stop the ping command on Host-11 and re-issue the command again, notice that the ping is working and the ISP router is receiving the packets with the public IP address of the router rather than the private IP address of the host itself.

Repeat the same command from host-12 and notice that the router is receiving the packets from the Host-12 with the gateway public IP address too.

In a way, the ISP router cannot tell which host is sending these packets.

Try fetching the web page from the web server using wget

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

  ```
  wget http://100.100.100.2/index.html
  ```

  What is the result ?

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

  ```
  wget http://100.100.100.2/index.html
  ```

  What is the result ?

6 Submission

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

```
stoplab sparta-pat
```

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.