Stateless Firewall Rules and VirtualBox Setup

Prepare VirtualBox Images

Start VirtualBox and Change the MAC Address

1. Open VirtualBox.
2. Navigate to **Settings > Network > Adapter 1 > Advanced > MAC Address**.
3. Generate a new random MAC address.

Change the Network Adapter

- **Home Network or University Ethernet Network**:
  - Go to **Settings > Network > Adapter 1**.

- Set **Attached to: Bridged**.

- **Eduroam (or other networks where Bridged is not feasible)**:

  1. Connect your laptop to a university ethernet network and set networking to **Bridged**.
  2. Alternatively, create a new NAT network:
     - Go to **File > Preferences > Networks > NAT Networks**.
     - Add a new NAT network, leaving all settings as default.
     - Set **Adapter 1** to use the NAT network you just created.

Start and Configure Ubuntu Image

1. Start the image and log in as `isp/isp`.

Disable IPv6

Since `iptables` supports only IPv4:

1. Open the file `/etc/sysctl.conf`.

2. Add the following lines at the end of the file:

   ```
   net.ipv6.conf.all.disable_ipv6 = 1
   net.ipv6.conf.default.disable_ipv6 = 1
   net.ipv6.conf.lo.disable_ipv6 = 1
   ```

3. Activate changes:

   ```
   sudo sysctl -p
   ```

   - The terminal should output the lines you added.
   - This command must be run each time the image starts; IPv6 is enabled by default at startup.

4. Verify IPv6 is disabled:

```
cat /proc/sys/net/ipv6/conf/all/disable_ipv6
```

- Output should be `1`.

Install Required Packages

Install packages used for testing firewall rules:

```
sudo apt-get install openssh-server apache2 curl git
```

Configure Apache2

1. Generate default digital certificates for Apache2:

   ```
   sudo make-ssl-cert generate-default-snakeoil --force-overwrite
   ```

2. Enable Apache2 SSL site:

   ```
   sudo a2ensite default-ssl
   ```

3. Enable Apache2 TLS/SSL module:

   ```
   sudo a2enmod ssl
   ```

4. Restart the Apache server:

   ```
   sudo service apache2 restart
   ```

5. Test Apache2:
   - Open a web browser and check both:
     - `http://localhost`
     - `https://localhost`

- Alternatively, test with `curl`.

Test SSH Server

1. Test by running:

```
ssh localhost
```

   - Answer `yes` and provide the password: `isp`.
   - Press `Ctrl+D` to exit.

Clone the Image

1. Shut down the guest:

```
sudo poweroff
```

2. In VirtualBox, right-click the image and select **Clone (Ctrl+O)**.
3. Choose **Expert Mode**:
   - Give the cloned image a name (e.g., `isp-2`).
   - Select **Linked Clone**.
   - Enable **Reinitialize the MAC address of all network cards**.
   - Click **Clone**.

Run the Images

1. Start both images.
2. Disable IPv6 on both images by running:

```
sudo sysctl -p
```

Test Connectivity Between Machines

1. Run `ip addr` on both machines to find their IP addresses.
2. Test connectivity using:

```
ping <ip_addr>
```

Download the Script Template

1. Download the script template by cloning the repository:

```
git clone https://github.com/lem-course/isp-iptables.git
```

   - If you get an error, install the git client first:

```
sudo apt install git
```

2. Change the downloaded file's execution permissions:

```
chmod +x iptables1.sh
```

Solve Assignments and Test Solutions

1. Follow instructions in the script to solve assignments.
2. Test each solution to verify it works.

Testing Steps

1. Start the firewall rules script:

```
sudo ./iptables1.sh start
```

   - To reset rules to default:

```
sudo ./iptables1.sh reset
```

2. Inspect activated rules:

```
sudo iptables --list -vn
```

   - Understand the output.

3. Test the rules using appropriate programs:

   - **ICMP**: `ping`
   - **DNS**: `dig`, e.g., `dig www.fri.uni-lj.si`
   - **HTTP**: `curl`, e.g., `curl google.com`
   - **SSH**: `ssh isp@<ip_of_target_machine>`

Typical Workflow

1. Solve a task.
2. Start or restart the firewall rules script:

```
sudo ./iptables1.sh start
sudo ./iptables1.sh restart
```

3. Inspect the rules:

```
sudo iptables --list -vn
```

4. Test using the appropriate program (e.g., `ping`, `dig`, `curl`, `ssh`).
5. Reset the rules if needed:

```
sudo ./iptables1.sh reset
```