Exercise 15.2: Enable a firewall which blocks all unwanted traffic

- Ensure SSH traffic is allowed.
- Ensure returning outbound traffic is allowed.
- Ensure all traffic on the loopback interface is allowed.
- Ensure all other traffic is blocked with `DROP`.
- Ensure the firewall rules persist through a reboot.

Solution 15.2

1. Allow all loopback traffic:

```
$ iptables -A INPUT -i lo -j ACCEPT
```

2. Allow all returning traffic:

```
# iptables -A INPUT -m state --state=ESTABLISHED,RELATED -j ACCEPT
```

3. Allow inbound SSH traffic:

```
# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

4. Block all other traffic:

```
# iptables -P INPUT DROP
```

5. Save your firewall rules:

   - On **CentOS**:

     ```
     # service iptables save
     ```

   - On **OpenSUSE**, the easiest way to save persistent firewall rules is to use the **YaST** tool.
   - On **Ubuntu**:

     (a) Install the package `iptables-persistent`.

     (b) Run this command to store the current rules:

     ```
     # iptables-save >/etc/iptables/rules.v4
     ```

