Building iptables rules

Set a default policy to drop packets:

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

Flush the previous rules:

```
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
```

Append rules:

```
iptables --append (CHAIN) (selection-criteria) --jump (TARGET)
```

or

```
iptables -A (CHAIN) (selection-criteria) -j (TARGET)
```

ACCEPT packets for specified ports, for example, `tcp/25`:

```
iptables -A INPUT  -p tcp --dport 25 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 25 -j ACCEPT
```

ACCEPT packets from specified subnets:

```
iptables -A INPUT  -s 192.168.122.0/24 -j ACCEPT
iptables -A OUTPUT -d 192.168.122.0/24 -j ACCEPT
```

Stateful inspection for TCP connections:

```
-m state
--state:  INVALID
          NEW
          ESTABLISHED
          RELATED
```

For example, to allow access to port `tcp/80` on Apache web server from subnet `192.168.122.0/24` only:

```
iptables -A INPUT -m state -p tcp --dport 80 -s 192.168.122.0/24 --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state -p tcp --sport 80 -d 192.168.122.0/24 --state ESTABLISHED,RELATED -j ACCEPT
```