Linux hardening: IP tables

As a system engineer your expertise is asked to create a firewall ruleset for a hosting server.The server is provided with the following services: Apache, ProFTPd and bind9. Please, do not allow zone transfers. Also protect the server against ping flooding. The server is not allowed to make outgoing connections, except for the installation of security updates.

DNS

```
iptables -A INPUT -p udp --dport 53 -j ACCEPT
iptables -A INPUT -p tcp --dport 53 -j DROP
```

The first line lets regular DNS traffic pass through. The second one makes sure we don't allow zone transfers, since this uses the TCP protocol.

ICMP

```
iptables -t filter -A INPUT -p icmp --icmp-type echo-request -m limit --
limit 5/minute -j ACCEPT
iptables -t filter -A INPUT -p icmp -j DROP
iptables -t filter -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

To protect the server against ICMP flooding we'll only allow 5 echo requests per minute. After that they will be dropped. Echo replies will be allowed.

Security updates

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -p tcp --dport http
-j ACCEPT
```

We will allow the server to install security packages. Established or related web communication will be allowed.

Result

Anything which doesn't follow these specific rules will be dropped. Our ruleset looks like this:

```
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
DROP       tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request limit: avg 5/min burst 5
DROP       icmp --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             state RELATED,ESTABLISHED tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-reply
```

```
-P INPUT DROP
-P FORWARD ACCEPT
-P OUTPUT DROP
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 53 -j DROP
-A INPUT -p icmp -m icmp --icmp-type 8 -m limit --limit 5/min -j ACCEPT
-A INPUT -p icmp -j DROP
-A INPUT -p tcp -m state --state RELATED,ESTABLISHED -m tcp --dport 80 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
```