Simple iptables Firewall

```
#!/bin/bash

# Set default policy
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Flush existing rules
iptables -F -t nat
iptables -F -t mangle
iptables -F -t filter
iptables -X

# Allow localhost traffic
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Allow related traffic
iptables -A INPUT -m conntrack --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m conntrack --state ESTABLISHED -j ACCEPT

# Allow icmp traffic
iptables -A INPUT -p icmp -j ACCEPT
iptables -A OUTPUT -p icmp -j ACCEPT

# Allow outgoing traffic
iptables -A OUTPUT -j ACCEPT

# Log & Drop the rest
iptables -A INPUT -j LOG --log-prefix "INPUT "
iptables -A INPUT -j DROP
iptables -A FORWARD -j DROP
iptables -A FORWARD -j LOG --log-prefix "FORWARD "

# Show ruleset
iptables -L -vnx
```

kb, linux, iptables, firewall, network