iptables cheat sheet

Notes:

1. All rules are processed from top to down. Once a rule is matched, the rest will be ignored.
2. Never run iptables -F if the default rules are DROP or your system will be inaccessible. If possible, set the default rule to ACCEPT and add iptables -A INPUT -j DROP at the end.

List all rules

```
iptables -L -n -v --line-numbers
```

Flush all chains (-F) and delete all user-defined chains chains (-X)

Note: Please ensure the default policy is ACCEPT or leave a ssh terminal before issuing

```
iptables -F
iptables -X
```

Set default policy

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

Block incoming ip address

```
iptables -A INPUT -s aa.bb.cc.dd -j DROP
```

Block outgoing sites

```
iptables -A OUTPUT -p tcp -d www.microsoft.com -j DROP
```

Allow ping from specific ip's only

```
iptables -A INPUT -s 1.2.3.0/24   -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

Allow ssh from specific ip's only

```
iptables -A INPUT -s 1.2.3.0/24   -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j DROP
```

Block incoming web access

```
iptables -A input -p tcp --dport 80 -j DROP
```

Port forward

Forward incoming connection to another internal host (aa.bb.cc.dd:22)

```
iptables -t nat -A PREROUTING -I eth0 -p tcp --dport 1022 -j DNAT --to aa.bb.cc.dd:22
iptables -A FORWARD -p tcp -d aa.bb.cc.dd -dport 22 -m state --state NEW,ESTABLISH -j ACCEPT
```

Delete a rule

```
iptables -L -n -v --line-numbers
iptables -D input {line-number}
```