iptables “cheat sheet” - For your convenience!

General command syntax:
`iptables` *`command`* `CHAIN` **`options`** *`action`*

Commands:
`-L` → List all currently inserted rules
`-F / --flush` → Delete all rules currently inserted
`-A` → “Append”: add a rule to a specific chain

Chains:
`INPUT` → Chain for packets targeted to your machine
`FORWARD` → Chain for packets that your machine will route
`OUTPUT` → Chain for packets that your machine sends out

`--policy CHAIN DROP/ACCEPT` → Set default behaviour for a chain

Options:
`-d / -s` → Filter by destination/source IPs
`-p TCP` → Filter TCP packets
`--dport / --sport #/name` → Filter by port # (or service, such as http, ssh...)
`--tcp-flags ALL` *`FLAG`* → Filter by flag. `ALL` means “inspect all packets”, substitute *`FLAG`* with the flag you want to filter

`-m` *`MODULE`* → Load an extension (for this lab: `string`/`state`)
`--string` *`“pattern”`* → Match *`“pattern”`* in packets
`--algo bm` → Use Boyer-Moore for pattern matching
`--state` *`OPTION`* → Filter by connection state. Can be `NEW`, `RELATED`, `ESTABLISHED` or `INVALID`

Actions:
`-j DROP/ACCEPT` → Action to take on matched packets