# Resumo do comando iptables

```
iptables [-t table] command [chain] [match] -j [target/jump]
```

Existem os seguintes "chains":

- INPUT
- OUTPUT
- FORWARD
- PREROUTING
- POSTROUTING
- User defined chains (just give it a new name instead of one of the pre-defined names)

Resumo das principais opções do iptables:

| --table<br>-t | Description |
|---|---|
| filter | Default table. This is used if not specified |
| nat | Network address translation |
| mangle | Used for Quality Of Service (QOS) and preferential treatment |

| Command (Use one) | Description |
|---|---|
| -A<br>--append | Append rule to chain |
| -D<br>--delete | Delete rule from chain |
| -I<br>--insert | Insert rule at beginning or at specified sequence number in chain. |
| -R<br>--replace | Replace rule |
| -F<br>--flush | Flush all rules |
| -Z<br>--zero | Zero byte counters in all chains |
| -L<br>--list | List all rules. Add option --line-numbers for rule number. |
| -N<br>--new-chain | Create new chain |
| -X<br>--delete-chain | Delete user defined chain |
| -P<br>--policy | Set default policy for a chain |
| -E<br>--rename-chain | Rename a chain |

| matches | Description |
|---|---|
| -s<br>--source | Source address of packet |
| -d<br>--destination | Destination address of packet |
| -i<br>--in-interface | Interface packet is arriving from |
| -o<br>--out-interface | Interface packet is going to |
| -p<br>--protocol | Protocol:<br>• tcp<br>--sport port[:port]<br>--dport port[:port]<br>--syn<br>• udp<br>• icmp<br>• mac<br>• ... |
| -f<br>--fragment | Fragment matching |
| -m state<br>--match state | --state<br>• ESTABLISHED<br>• RELATED<br>• NEW<br>• INVALID<br>(Push content, not expected to receive this packet.) |

| target/jump | Description |
|---|---|
| ACCEPT | Let packet through |
| DROP | Deny packet with no reply |
| REJECT | Deny packet and notify sender |
| RETURN | Handled by default targets |
| MARK | Used for error response.<br>Use with option --reject-with *type* |
| MASQUERADE | Used with nat table and DHCP. |
| LOG | Log to file and specify message:<br>--log-level #<br>--log-prefix "*prefix*"<br>--log-tcp-sequence<br>--log-tcp-options<br>--log-ip-options |
| ULOG | Log to file and specify userpace logging messages |
| SNAT | Valid in PREROUTING chain. Used by nat. |
| REDIRECT | Used with nat table. Output. |
| DNAT | Valid in POSTROUTING chain. Output. |
| QUEUE | Pass packet to userspace. |