Connection Tracking - 1

Connection Tracking = Stateful Firewall

- Connection tracking = ability to maintain **state information** about connections.
- Stateful firewalls are **more secure** than stateless firewalls.
- Stateful firewalls decide to accept or to drop packets **based on the relations** these packets are with other packets.
- Netfilter is a stateful firewall.

Connection Tracking - 2

Connection tracking = stateful firewall

Packet states:

1. NEW - the first packet from a connection.
2. ESTABLISHED - packets that are part of an existing connection.
3. RELATED - packets that are requesting a new connection and are already part of an existing connection (Ex: FTP).
4. INVALID - packets that are not part of any existing connection.
5. UNTRACKED - packets marked within the raw table with the NOTRACK target.

Connection tracking can be used even if the protocol itself is stateless (Ex: UDP, ICMP).

Connection Tracking - 3

-m state --state *state*, where state is a comma separated values of packet states written in UPPERCASE letters

Example:

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```