Configuring Firewall in Advanced Mode

- There are three control policies in the advanced mode firewall:
  accept the packet: if the packet is accepted, it gains access to the system drop the packet: if the policy is to drop the packet, the packet is denied access to the system reject the packet: the system does not let the packet in, notifying the sender of the fact

- These policies, along with ports and protocols, are called chains attributes. A chain is a list of rules grouped by the criterion of what type of packets they process.
  There are three packets types:
  inputoutput forward

Thus you can create three chains - the Input chain, the Output chain and the Forward chain.
The Input chain examines the incoming packets. If there is a rule to process a packet, the latter is either let in (accept policy) or not (drop/reject policy). Otherwise, the packet is examined by the next rule. If, finally, there is not any rule to match, the default system policy is applied. The first rule applied to a packet is the first one on the list that forms a chain.
If a packet is created inside the system, it is sent to the Output chain. Packets that pass through the system, traverse the Forward chain. When configuring a firewall, you can change a rule's position on the list, delete a rule from the list, create, edit and add rules to the list.
Activating the Advanced Mode:
1. Login to your Parallels Power Panel.
2. Click on the Firewall link.
3. If your firewall is currently inactive, activate it in the Advanced Mode. If your firewall is currently in the Normal mode, switch it to the Advanced mode via the Firewall Setup icon.

https://kb.in2net.net/questions/65/