PkgMaster.com How-To's

Qube3 Firewall How-To

This is a step by step document for anyone who wants to set up the basic firewall feature on their Qube3. This HOW-TO intends to explain a few basic things about firewalls and port access.

All communication between two computers hapens via logical connections named ports. Below is a list of the port numbers that certain well known communication protocols use.

Protocol	Port number
FTP	21
SSH	22
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110
IMAP	143
SSL	443

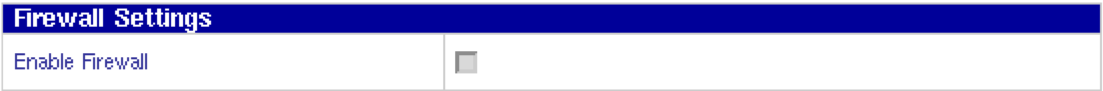
In order to allow or disallow anyone to be able to connect via a protocol, the corresponding port needs to be open or closed. Besides these ports, some other ports need to be open in order to have certain protocols work properly. Both DNS and HTTP make requests at the ports in the list, but get a response on a random port in the range of 1025 to 66535. So to have HTTP or DNS work properly, these ports also need to be open!

The Cobalt OS needs another two ports to be open in order to have the webinterface work properly. The main port is port 81, the emergency port is port 444. The Qube firewall will detect if these ports are open and if not, the firewall will be shut down.

So, how do we set up the firewall? There is a whole lot that can be said about this and I guess everyone will have their own demands on what ports to open and what not. I'll just breifly go through all the options in the webinterface and explain what they are for. You decide on which ports to leave open and which ones not.

Step 1

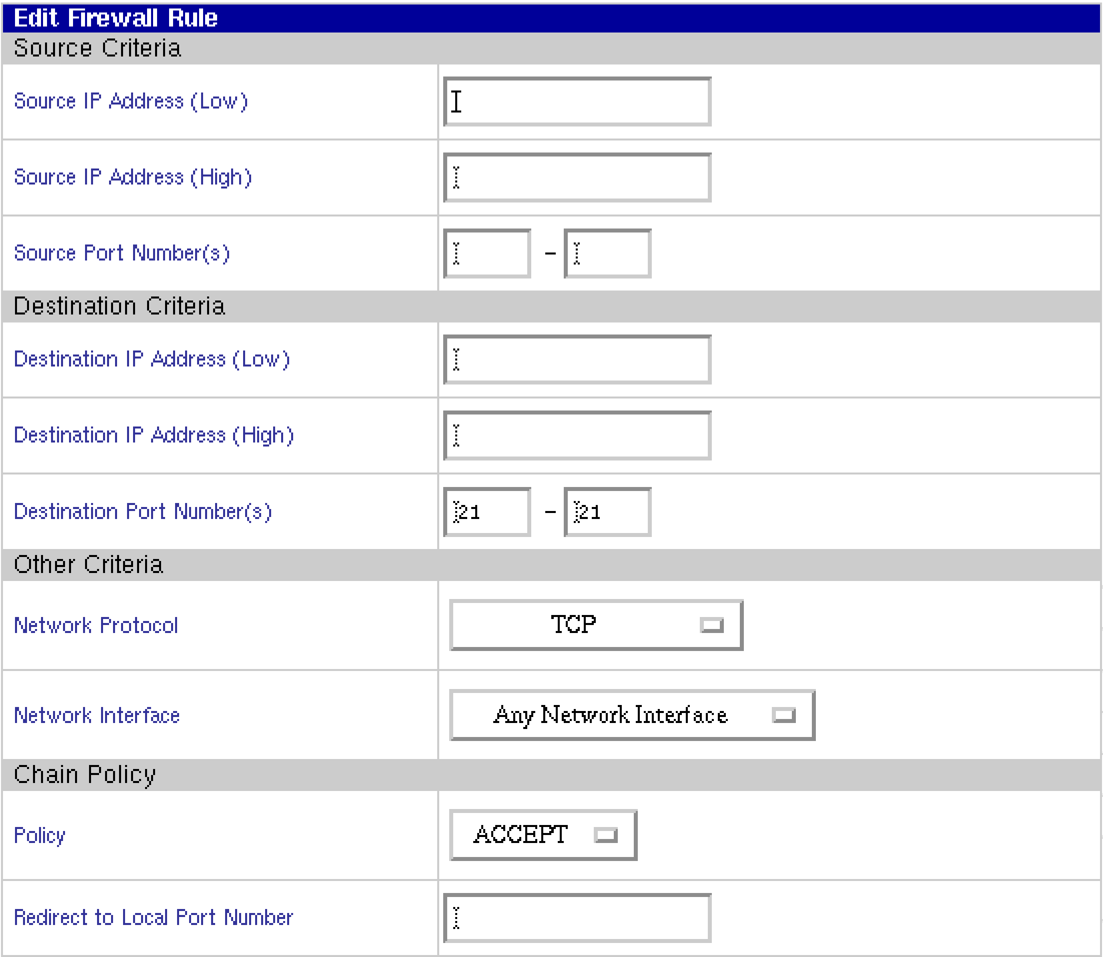
Of course the firewall needs to be switched on.



Firewall Settings	
Enable Firewall	□

Step 2

First I'll show you what al the input fields in the Edit Firewall Rule page mean :



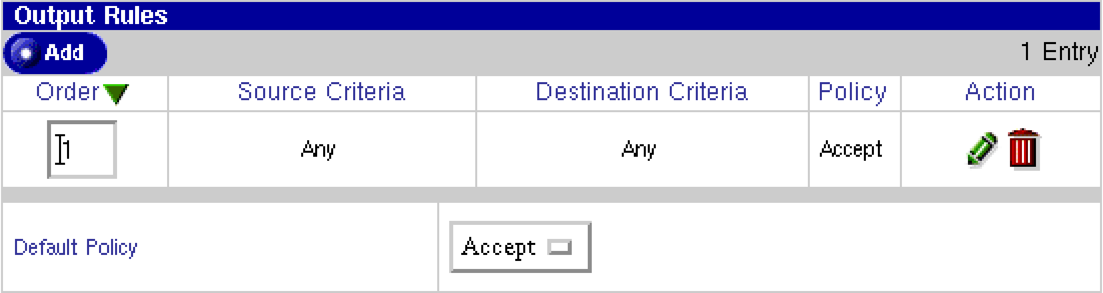
Edit Firewall Rule	
Source Criteria	
Source IP Address (Low)	
Source IP Address (High)	
Source Port Number(s)	-
Destination Criteria	
Destination IP Address (Low)	
Destination IP Address (High)	
Destination Port Number(s)	21 - 21
Other Criteria	
Network Protocol	TCP
Network Interface	Any Network Interface
Chain Policy	
Policy	ACCEPT
Redirect to Local Port Number	

With the first two boxes you can specify the ip range for which this rule applies. Leaving them empty means : all ip addresses. If you only need one ip address, add that one in both boxes. The same applies for the port numbers. For the destination criteria the same applies.
The Network protocol is a different story. You can specify if the rule applies to TCP, UDP or both. The main difference between TCP and UDP is that TCP ensures communication between two applications on both sides of the line, while UDP just receives a request and sends one back. It doesn't care who listens to it.
The Network Interface selects for which network interface the rule applies. If you're closing ports, you only want the rule to apply for the primary (i.e. external) network interface.
The Policy selects if a connection to the port specified above is accepted or denied. Closing a port means denying a connection.

If you use the firewall as ip chain you can specify a destination port in Redirect to Local Port Number.

Step 3

Now you need to decide which ports you want to close and which to leave open. If you want the computers in your LAN to have full access to the internet, don't specify any outgoing rules, like this :



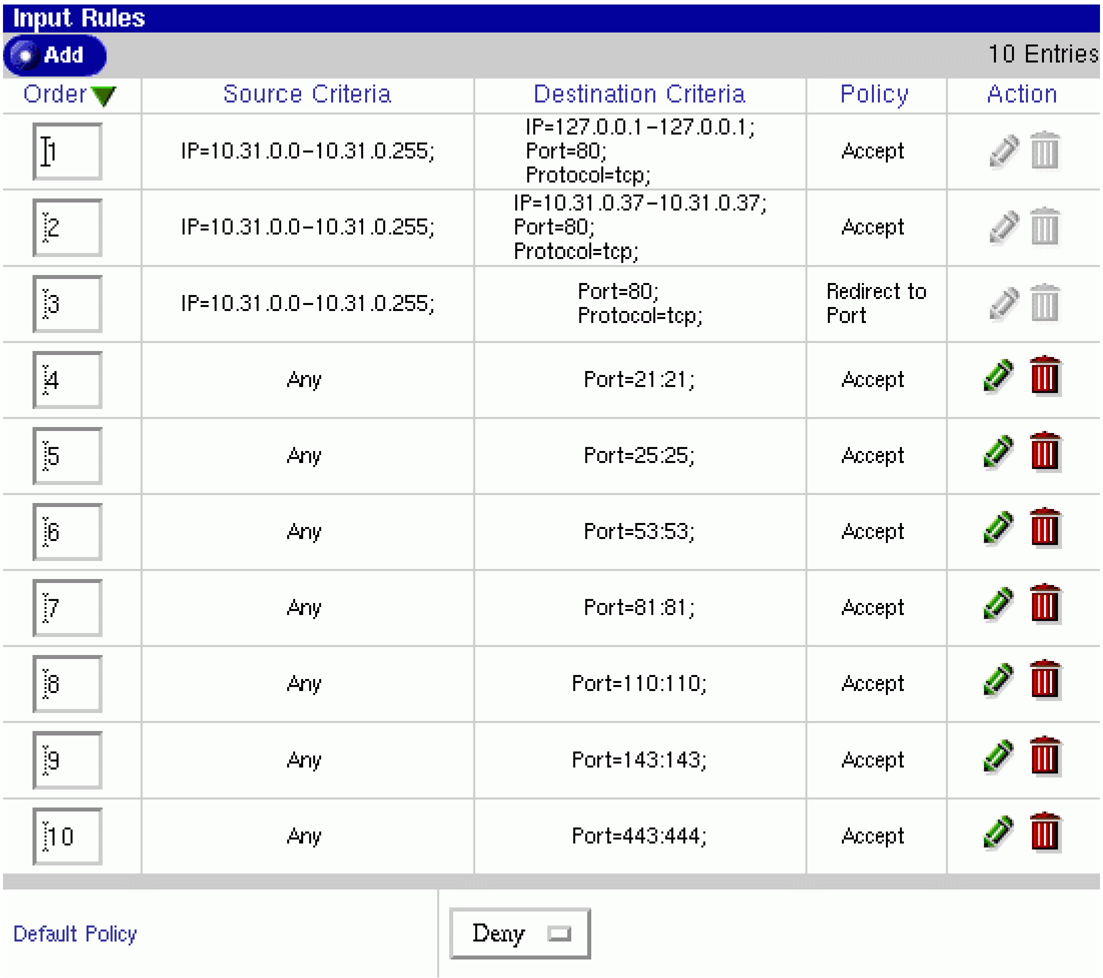
Output Rules

1 Entry

Order	Source Criteria	Destination Criteria	Policy	Action
1	Any	Any	Accept	✎ 🗑

Default Policy: Accept

To open or close any ports for the outside world, set up something like this :



Input Rules

10 Entries

Order	Source Criteria	Destination Criteria	Policy	Action

1	IP=10.31.0.0-10.31.0.255;	IP=127.0.0.1-127.0.0.1;
		Port=80;
		Protocol=tcp;
			Accept	✎ 🗑

2	IP=10.31.0.0-10.31.0.255;	IP=10.31.0.37-10.31.0.37;
		Port=80;
		Protocol=tcp;
			Accept	✎ 🗑

3	IP=10.31.0.0-10.31.0.255;	Port=80;
		Protocol=tcp;
			Redirect to Port	✎ 🗑

4	Any	Port=21:21;	Accept	✎ 🗑
5	Any	Port=25:25;	Accept	✎ 🗑
6	Any	Port=53:53;	Accept	✎ 🗑
7	Any	Port=81:81;	Accept	✎ 🗑
8	Any	Port=110:110;	Accept	✎ 🗑
9	Any	Port=143:143;	Accept	✎ 🗑
10	Any	Port=443:444;	Accept	✎ 🗑

Default Policy: Deny

Since the default policy here is to DENY any connections, all attempts to connect to the Qube on any port not in the list are rejected. Please note that the above image doesn't show all the possibilities. Also, the first three rules are put there automatically if you enable webcaching.