Blocked IP Addresses

Over time, you may find unauthorized clients attempting to gain access to your server. This may be due to malicious people intentionally attacking your server or virus-infected computers randomly blasting any server they can find. In either case, the most efficient and secure way to handle such clients is to block their incoming connection requests as soon as they are detected.

Note that other access restrictions, most notably user authentication by password, will generally be very effective at keeping out intruders, making blocked addresses somewhat redundant. However, blocking unruly clients as soon as they are detected does reduce overhead (since the server does not need to prompt for, accept, and verify the username and password) and removes the possibility (as slim as that may be) that the hacker will guess a password. To completely eliminate the overhead involved in processing hack attempts, and to protect other computers on your network from the trouble-making client, configure your router to block the address from accessing your entire network.

The "Blocked IPs List" is a simple list of client IP addresses. To add an address, click the Add icon (the "plus") sign. A sheet will drop down, allowing you to supply the address that should be added to the list. To remove an entry, select the entry in the list and click the Remove icon (the "minus" sign).

Specifying Entire Subnets

An entire subnet can be added to the list, allowing you to quickly block an entire network from accessing your server. To add a subnet, click the Add icon, then specify the first 3 numbers of the subnet address, with "0" as the fourth. For example, an entry of "192.168.1.0" would block all server access from any computer on the subnet "192.168.1.".

Automatic Detection Of Hack Attempts

Rumpus can be set to identify client computers that are attempting to guess passwords, and add those client addresses to the list automatically. Control of this feature is provided on the "Security" tab of the "FTP Settings" window.

Deny Addresses NOT In This List

If you are particularly security conscious, and know that FTP clients will be accessing your server from a fairly restricted number of computers, you can decide to block all access to the server except by clients from known addresses. In other words, rather than listing bad clients and allowing access to everyone else, you can set Rumpus to restrict access to everyone, unless they appear in a list of known good clients.

By checking the "Deny Addresses NOT In This List" option, you essentially reverse the behavior of the list so that only clients with an address that appears in the list will be allowed to access the server. For example, if your server is intended for local use only, and your local subnet is "192.168.1.", then checking this option and adding "192.168.1.0" will block any access attempts by any computer not on your local network.

Note that enabling this option essentially disables the Rumpus automatic hack attempt detection, since all addresses will automatically be denied except for those you specifically list as known good addresses.