

Firewall Setup

Configuring the Mac OS X firewall to allow FTP and WFM connections.

Getting Started

The basic job of the OS X firewall is to block unwanted network access to your computer, so when your firewall is enabled, it will need to be configured to allow external users to connect to Rumpus FTP and Web services. When you are just getting started with Rumpus, it is usually best to temporarily disable the firewall, eliminating the possibility that it will interfere with service. Once you have confirmed that your Rumpus server is running and available, the firewall can be re-enabled and setup as needed.

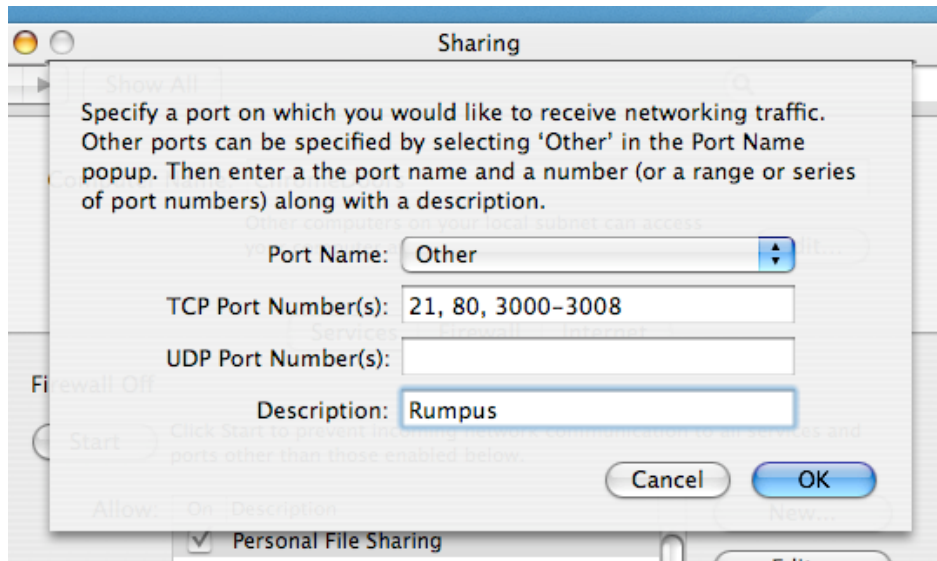
To disable the OS X firewall, open the System Preferences window and select the “Sharing” panel, then switch to the “Firewall” tab and click the “Stop” button. FTP and Web services should now be accessible to other computers on your LAN, and the Internet in general when your network is configured properly.

Configuring The Firewall

Rumpus can be run indefinitely with the firewall off, but for better server security it is usually a good idea to use the firewall to restrict access to explicitly allowed services. To enable the firewall, click the “Start” button on the “Firewall” tab of the Sharing System Preferences panel.

To enable incoming connections to Rumpus, you will need to allow access to the FTP control port, FTP data ports, and the Web File Manager port. By default, these are ports 21, 3000-3008 and 8000, although port 80 is very commonly used instead of 8000 for the Web File Manager. To confirm the ports needed, check the “FTP Port Number” on the “Basics” tab of the FTP Settings window, the “Passive Mode Port Range” on the Advanced tab of the FTP Settings window, and the “Port Number” field of the Web Settings window.

On the Firewall tab of the Sharing panel, click the “New...” button to create a new entry in your firewall setup. On the sheet that opens, set the “Port Name” to “Other”, the “Port Number” to “21, 80, 3000-3008” (or whatever the required port values are) and the “Description” to “Rumpus”, as shown in the image below:



When you click “OK”, you will notice that the entry “Rumpus” has been added to the “Allow” list. The entry should be checked automatically, but if it isn’t, be sure to enable the rule by checking the box in the “On” column.

With the firewall on and the “Rumpus” entry created, you should now be able to access your Rumpus server while the OS X firewall blocks access to all other restricted ports. If you have trouble connecting to the server from another computer on your LAN after completing this procedure, be sure to contact Maxum Technical Support at “support@maxum.com”.

SSL Encrypted Sessions

If you have enabled SSL tunneling to provide FTPS and/or HTTPS sessions, additional ports will need to be permitted, in addition to the basic FTP and HTTP ports. The process is identical to that described above; just create a new entry on the firewall setup tab, specify the necessary ports and port ranges, and assign a clear description, such as “Rumpus SSL”. If you prefer, the necessary SSL ports can simply be added to the list in the primary Rumpus firewall entry.

The ports that need to be allowed for SSL sessions are typically 990 (FTPS control connections), 443 (HTTPS connections) and the range 4000-4008 (FTPS data connections). While not generally recommended, the HTTPS port can be changed on the “Advanced” tab of the Web Settings window, and the firewall setting needs to match the selection in Rumpus. The FTPS data connection range is also selectable, and is always the standard FTP passive mode data connection range, plus 1000. So, for example, if you have set Rumpus to allow 20 simultaneous FTP sessions, making the standard passive mode port range 3000-3020, the FTPS passive mode port range would be 4000-4020.

In some cases, only SSL encrypted sessions should be allowed when connecting to a server. To disallow standard FTP and HTTP connections, create a firewall entry that includes only the SSL ports, without the standard 21, 80 and 3000-3008 ranges. With the OS X firewall enabled, but only SSL-encrypted ports opened, only secure sessions will be allowed.