



Firewall Setup

Contents

| | |
|---|----------|
| Getting Started | 2 |
| Running A Firewall On A Mac Server | 2 |
| Configuring The OS X Firewall | 3 |
| Remote Rumpus Administration | 4 |
| Firewall Setup Under OS X 10.4 | 4 |

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 "Security" panel, then switch to the "Firewall" tab and choose the "Allow all incoming connections" option. (In OS X 10.6, simply use the "Stop" button to stop the firewall, if it is running.) 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.

Running A Firewall On A Mac Server

Mac OS X 10.5 and later includes an application based firewall, which accepts or blocks incoming connections to your server based on the application that is set to receive the request. For typical OS X client applications, this makes sense and simplifies firewall setup. However, on a Mac run as a server, a port based firewall is more flexible and secure.

Using a port based firewall allows you to choose which specific ports will be accessible to outside users, and allows you to deny access to any service not run on an explicitly permitted port. For the purposes of a file transfer server, a port based firewall simplifies setup, clarifying exactly what connections should be allowed or blocked.

There are a number of good 3rd party firewalls available. We recommend DoorStop, from Open Door Networks (<http://www.opendoor.com/doorstop/>), which offers a straightforward interface, is very reliable, and is reasonably priced.

When using DoorStop, or any port based firewall, configure the firewall so that all ports are blocked, and then explicitly allow the necessary ports as described on the "Network Setup" window in Rumpus.

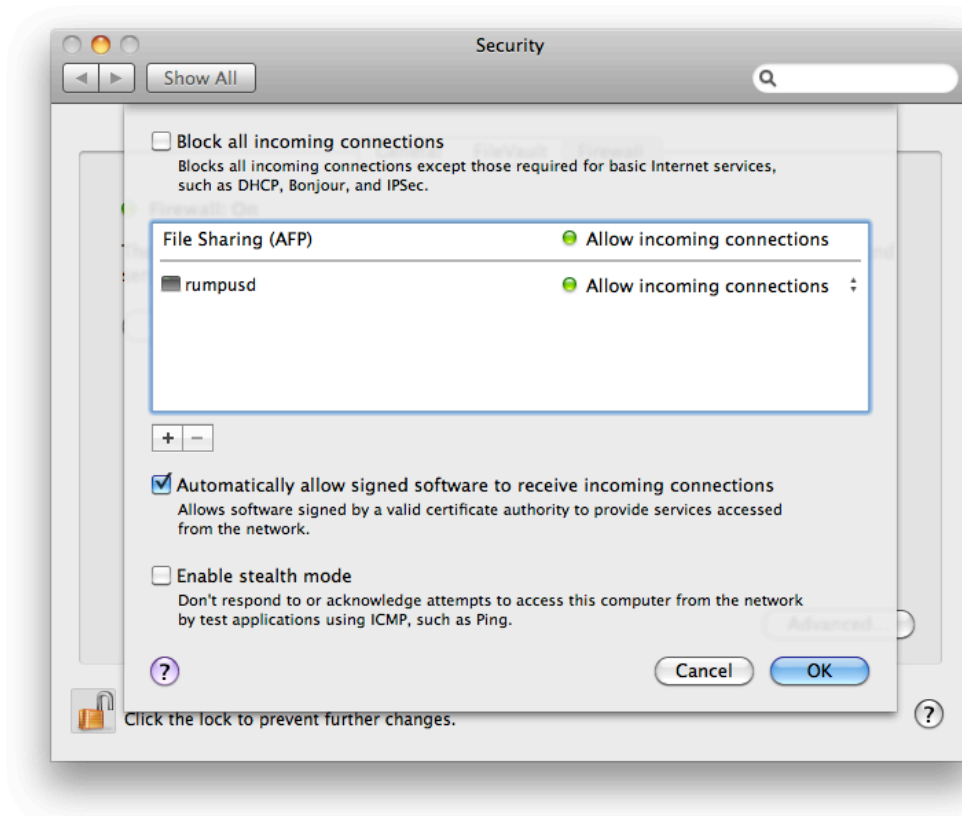
Configuring The OS X Firewall

While a 3rd party firewall is the better option (as described above), Rumpus can be run with the OS X built-in firewall. To configure the firewall, open the “Security” System Preferences panel and flip to the “Firewall” tab. (In OS X 10.6, you will then need to click the “Advanced...” button on the Firewall tab to access the firewall setup options.) Choose the “Set access for specific services and applications” option (OS X 10.5) or check the “Automatically allow signed software to receive incoming connections” box (OS X 10.6) to set the firewall to allow incoming connections by application.

To enable incoming connections to Rumpus, you will need to allow inbound connections to the Rumpus server daemon. To begin, select “Open Config Folder” from the “File” menu in Rumpus. This will open the Rumpus configuration folder, which is normally hidden in the Finder and contains the Rumpus daemon application.

Next, on the “Firewall” tab of the Security System Preferences panel, click the “Add” button to add an accessible service. When the standard file selection sheet drops down, drag the “rumpusd” application from the Rumpus configuration folder into the file listing on the sheet. This will cause the “rumpusd” file to be selected automatically, and you can then complete the sheet.

Make sure that the rumpusd application is added to the list of accessible services, and is set to “Allow incoming connections”, as shown below:



With the firewall on and the “rumpusd” 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”.

Remote Rumpus Administration

The “Rumpus Remote Daemon” allows the Rumpus application to be run from remote Macs, if necessary. The remote daemon will also need to be added to the list of applications that are allowed to accept incoming connections, if you decide to enable Rumpus remote management.

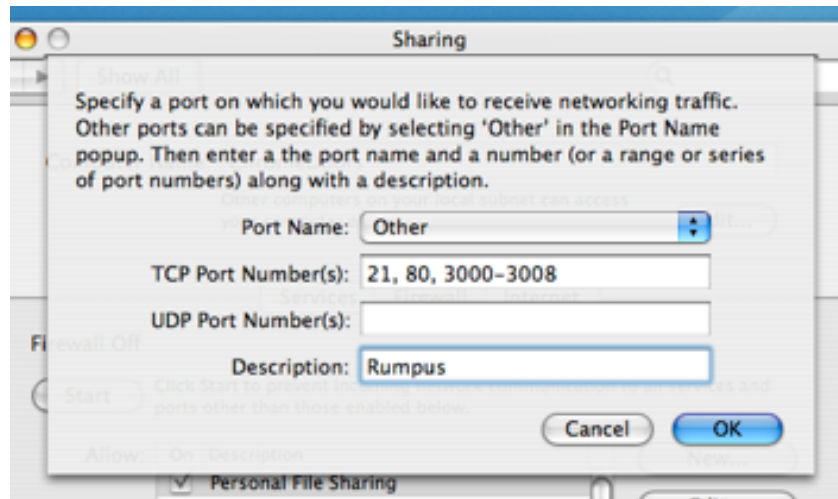
The Rumpus remote daemon is called “rumpusremoted” and resides in the same Rumpus configuration folder as the main rumpusd daemon. It can be added to the list of applications allowed to receive connections in exactly the same way the rumpusd daemon was added.

Firewall Setup Under OS X 10.4

To access firewall setup under OS X 10.4, open the System Preferences window and select the “Sharing” panel, then switch to the “Firewall” tab.

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 80, although port 8000 may be used instead of 80 for the Web File Manager. To confirm the ports needed, check the information on the “Router” tab of the “Network 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”.