**Command Line ALF on Mac OS X**

Mac OS X 10.5 and Mac OS X 10.6 have a multitude of ways to keep data from coming or going from a system. The traditional way is to use ipfw, although this isn’t the default way in 10.5 and above. Instead, you are meant to use the Application Layer Firewall (we’ll call it ALF for short), which is what you configure from the Security System Preference pane. You can enable the firewall simply enough by using the defaults command to augment the /Library/Preferences/com.apple.alf.plist file, setting the globalstate key to an integer of 1:

*defaults write /Library/Preferences/com.apple.alf globalstate -int 1*

You can also configure the firewall from the command line. Stopping and starting ALF is easy enough, whether the global state has been set to 0 or 1, done using launchd. To stop:

*launchctl unload /System/Library/LaunchAgents/com.apple.alf.useragent.plist launchctl unload /System/Library/LaunchDaemons/com.apple.alf.agent.plist*

To start:

*launchctl load /System/Library/LaunchDaemons/com.apple.alf.agent.plist launchctl load /System/Library/LaunchAgents/com.apple.alf.useragent.plist*

These will start and stop the firewall daemon (aptly named firewall) located in the /usr/libexec/ApplicationFirewall directory. As you can imagine, the settings for ALF can be configured from the command line as well. The socketfilterfw command, in this same directory, is the command that actually allows you to manage ALF. ALF works not by the simple boolean means of allowing or not allowing access to a port but instead by limiting access by specific applications, more along the lines of Mandatory Access Controls (although not yet using the MAC framework). When an application is allowed to open or accept a network socket, it’s known as a trusted application – and ALF keeps a list of all of the trusted applications. You can view trusted applications using socketfilterfw with the -l option; although the output can be difficult to read and so you can constrain it using grep for TRUSTEDAPPS as follows:

*./socketfilterfw -l | grep TRUSTEDAPPS*

You can also use the command line to add a trusted application using the -t option followed by the path to and then the actual application to be trusted. For example, to add FileMaker to the list of trusted apps you use something similar to the following, pointing to the binary, not the app bundle:

*./socketfilterfw -t “/Applications/FileMaker Pro 9/FileMaker Pro.app/Contents/MacOS/FileMaker Pro”*

Note: You can also use the socketfilterfw command to sign applications, verify signatures and enable debugging, using the -s, -v options and -d options respectively. Finally, there are a number of global preferences for the firewall that can be configured using the /usr/libexec/ApplicationFirewall/com.apple.alf.plist preferences file. You might be looking at the path to this file and thinking that it looks odd and it should really be in /Library/Preferences. And you might be right. But the com.apple.alf.plist file there appears to be a bit of silly misdirection. Changes there simply don’t seem to have the desired response. Therefore, stick with the one in the /usr/libexec/ApplicationFirewall directory. Some keys in this file that might be of interest include globalstate (0 disables the firewall, 1 configs for specific services and 2 is for essential services – as in the GUI), stealthenabled and loggingenabled. All are integers and fairly self explanatory vs. GUI settings from the System Preference pane.