TCP Flow ReadMe
18 November 2002

"tcpflow" is a common unix tool for capturing the contents of TCP data connections.

This version of IPNetSentryX includes an option in the TCP Dump window to "Use tcpflow" instead of tcpdump. Using tcpflow makes it easier to examine TCP data content as opposed to packet headers.

To use TCP Flow, you will need to install the tcpflow package distributed with IPNetSentryX or available here: http://www.entropy.ch/software/macosx/. You can learn more about tcpflow here: http://www.circlemud.org/~jelson/software/tcpflow/tcpflow.1.html, and read more about unix tcpdump in the help text for the TCP Dump window. Under the Help menu, select IPNetSentryX Help (cmd-?) and then click on the link for the TCP Dump tool.

Some of you may have read recently about a corrupted version of "tcpdump" posing a security threat to unix systems.   It is important to obtain any privileged tools from a reliable source since you are trusting this code not to harm your data. IPNetSentryX uses the version of tcpdump already on your computer, which is normally installed as part of Mac OS X.   The version of tcpflow included with IPNetSentryX is a port of the corresponding unix tool obtained from the website above.   To the best of my knowledge, these are reliable ports of open source unix tools.

Enjoy!

- Peter Sichel
   Sustainable Softworks