IPNetSentryX ReadMe

Product page: <http://www.sustworks.com/site/prod_sentryx_overview.html>
24 Mar, 2004

README CONTENTS

---

1. Introduction

IPNetSentryX is an advanced firewall, intrusion detector, that includes detailed logging, Ethernet bridging, bandwidth allocation, and bandwidth accounting.

Unlike most other Internet security products, IPNetSentryX does not erect barriers for the safe use of your Internet connection. There is no need to "punch holes" in a firewall for specific applications you may wish to run. Instead, IPNetSentryX silently and intelligently watches for suspicious behavior, and when triggered, invokes a solid filter which completely bans the potential intruder from your Macintosh.

If you prefer not to read detailed instructions, open the IPNetSentryX QuickStart ReadMe to begin using the software immediately.

---

2. Features

* Provides intelligent protection without expert configuration.
* Does not interfere with normal network operation or software.
* Hierarchical filter rules are easy to understand, efficient, and offer exceptional control over network traffic.
* Provides Bandwidth Allocation to improve network utilization.
* Provides Bandwidth Accounting to audit network usage.
* Provides Ethernet Bridging to create transparent firewalls.
* Includes AirPort configuration for setting up software base stations.

* Supports data content filtering to stop Internet worms.
* Safely ignores promiscuous TCP resets.
* Unique on screen updates show firewall rules in action.
* Includes tools to probe and examine network behavior.
* Flexible network event monitoring and Email notification.
* Full Macintosh user interface makes these tools more accessible.

The simple well organized display with built-in examples allow both new and experienced Internet users to benefit from a powerful firewall intrusion detector.
---

3. IPNetSentryX System requirements

MacOS X 10.2 (Jaguar) or later.
BSD subsystem installed

4. Installation and Removal

To install or remove the software, simply drag a copy to your hard drive. The first time IPNetSentryX is run it will ask you to authenticate to complete the installation process. Notice you must copy the software to your hard drive and then authenticate. IPNetSentryX will not run properly from a Read Only disk image since it requires UNIX privileges.

Under UNIX operating systems including Mac OS X, certain operations require special permission or privileges to prevent unauthorized users from disrupting or spying on other users. While well intentioned, these conventions are often inappropriate for a "personal" computer where a single user owns and administers the system. Among the operations that require such privileges are monitoring all network traffic.

IPNetSentryX takes the personal computer view that the user should normally be in control of their computer, so tries to minimize the disruption of asking the user to prove they are authorized to perform the requested operation.

To monitor network traffic, IPNetSentryX includes a tiny server application named "LoadNKE" that must run as suid root. When IPNetSentryX is first run after being copied to a new location, it checks to see if the LoadNKE tool is present and set to suid root. The same process is repeated for "RunTCPDump", and "RunTCPFlow". If any of these tools are not authorized, it asks you to authenticate so it can configure them to run as suid root. You might think of this as completing the installation process. From that point on, no further authentication is necessary to perform any of the restricted

operations IPNetSentryX supports.

Normally allowing small programs to execute as root is not a problem unless the program seeks to compromise your system or is exploited by another program to carry out such an attack. The best defense against such exploits at this time is to only run software from reputable developers. Future versions of Mac OS X will hopefully offer finer control over software privileges so it will no longer be necessary to open your entire system (by granting root privileges) to programs that need to perform legitimate specialized tasks.

When copying the IPNetSentryX application, you may see a warning message like this:

One or more items can't be copied. Do you want to skip them and copy the remaining items?

This message appears because the user performing the copy operation does not have sufficient privileges to retain the root ownership of items that have been set to suid root. Instead of creating new copies belonging to the user performing the copy, Apple chose to issue a warning message and not copy them at all. Under Mac OS X 10.1, IPNetSentryX is self repairing so you can simply press "continue" and re-authorize the copied version the next time it is run. Under Mac OS X 10.2 the entire IPNetSentryX application may fail to copy. In this case you can select "Unauthorize Tools..." under the IPNetSentryX menu to restore the file permissions to allow copying.

If you have trouble running IPNetSentryX from another hard disk volume, make sure you have not disabled privileges on this volume. Select the volume and do a "Get Info" (cmd-I). Choose "Privileges" from the popup menu and make sure "Ignore privileges on this volume" is unchecked. IPNetSentryX requires UNIX privileges for many of the tools to work.

IPNetSentryX uses a probe module (IPNetSentry_NKE) to intercepts network traffic while the Firewall is enabled. When the firewall is disabled, the probe module is automatically removed from the corresponding data stream. The NKE normally remains loaded until you restart your system since other applications might be using it. You can try forcing the NKE to unload by selecting "Unload NKE" from the IPNetSentryX application menu. This feature allows you to load a newer version of the NKE without restarting your system. The NKE will only unload when all monitoring connections to it have been stopped.

---

5. How to Get Started

If you prefer not to read detailed instructions, open the IPNetSentryX QuickStart ReadMe to begin using the software immediately.

To begin using IPNetSentryX, launch the application completing the installation process if necessary. A firewall document appears containing the default firewall configuration. Use the disclosure triangles along the left side of the outline to examine any rules in more detail. Option-Expand will expand all the rules beneath a single item.

When you are ready, press "Apply" to load your firewall rules to the network kernel and select "Enable Firewall". Congratulations, you now have basic firewall protection. You can watch as network traffic matching a firewall rule is detected (select "Match Count" under the Parameter PopUp) or check the Log to see suspected intruders being denied access. You can edit and "Apply" new rules at any time without restarting the firewall. Notice the IPNetSentryX application must be running for the firewall to be active (this may change in a future version). No windows need be open however.

Of course there is much more you can do.

Help is available on the various tools and features from the Help menu. This is probably the best way to familiarize yourself with the more advanced features of the software since you can experiment with the window while you read the description.

Notice some rules in the default configuration may be disabled. You can easily turn individual firewall rules on or off to experiment or satisfy more advanced requirements. To enable or disable individual firewall rules, use the corresponding checkbox in the left most column and press "Apply" to invoke your changes. You can save your customized settings as IPNetSentryX documents and invoke them automatically at login time or when your system starts up.

Once you are comfortable IPNetSentryX is working as desired, you can configure it to launch as a Mac OS X startup item outside the context of any user login. To do this, drag the IPNetSentryX application bundle to /Library/StartupItems. You can launch IPNetSentryX from the Finder and select "Tool->Filters/Interfaces" to see the currently running firewall status. If you encounter difficulty, you can restart while pressing the Shift key to prevent startup items from loading and then remove IPNetSentryX from the /Library/StartupItems folder.

---

6. IPNetSentryX Version History

See "Release Notes" under IPNetSentryX Help for version history including the latest features and additions.
---

7. Registration and Licensing

IPNetSentryX is commercial software subject to the terms of the accompanying License Agreement. You may use a demo version of the software during a single trial period of up to 21 days. You must then register the software if you wish to continue using it beyond the trial period.

Notice the trial is designed to expire after 21 days. If the software reports it has expired the first time you launch it, this usually means someone ran a previous version of the program on your computer. Please contact us directly for information on how to reset the trial period.

Once you have downloaded the application, there are 2 basic ways to register:

(1) Register on-line at <https://www.sustworks.com/cgi-bin/nr1.pl>

(2) For site license registrations, we can fax your company a proforma invoice. Please contact us directly at <mailto:admin@sustworks.com> .

The XML registration key that unlocks the demo startup screen and expiration will be sent to you by email once your registration information is received. You should simply paste the ENTIRE XML Key into the Registration Key field and click the "Accept" button. Your program is now registered. Thank You!

Pricing
- Single User $40
- Upgrade from IPNetSentry classic $20
- Price will increase to $60 ($30 upgrade) on August 22, 2005

Additional payment details are available on our registration web page at

<http://www.sustworks.com/site/reg.html>
---

8. Thank You!

We hope you find our IPNetSentryX software useful and look forward to your comments and suggestions.

support help <http://www.sustworks.com/site/sup.html>

registration issues <mailto:admin@sustworks.com>

other questions <mailto:info@sustworks.com>

or mail us at:

Sustainable Softworks
13 Fieldside DR
Cumberland, RI 02864 USA

[End of ReadMe]