IPNetSentryX Release Notes

http://www.sustworks.com

Nov 16, 2005 - IPNetSentryX 1.3
• Release as version 1.3
• Fix possible window server conflict when launched as a startup item.

Nov 10, 2005 - IPNetSentryX 1.3c9
• Fix bug in matching data content.
• Fix possible panic if connection table overflows.
• Restructure Attach and Detach NKE to improve logging and consistency.
• Improve locking model under Panther.
• Changed "Filters/Interfaces" to "Expert View".
• Restructure firewall document to support an alternative "Basic View".
• Update IPNetSentryX Help to include Automatic Failover, Source Aware Routing, Bandwidth Allocation, and other recent changes.

Sep 14, 2005 - IPNetSentryX 1.3c8
• User Interface: re-order tabs as Interfaces, Filters, Triggers.
• Enable the Apply button when there are changed settings to apply.
• Preferences: save preference settings to a common location regardless of user login.
• Fix checksum conflict by calling mbuf_inbound_modified on outbound packets to work around bug in mbuf_outbound_finalize() KPI.
• Save and restore source aware routing state consistently.
• Address Scan: work around bug in NSScanner.

Aug 26, 2005 - IPNetSentryX 1.3c7
• Add filter action "Route To" with parameter of next hop IP address for conditional routing.
• Save and re-use complete frame headers in connection table entry.
• Automatic failover: use split route as alternate default gateway.
• Fixed bug in converting SourceNet and DestNet IP address ranges.
• Fix to always disable alerts when launched as startup item.
• Filters: fix order when pasting a list of rules as children.
• Filters: add "authorize" rule to default firewall configuration.
• Filters: add sample "rate limiting" rules for PPP to default firewall configuration.

Jul 29, 2005 - IPNetSentryX 1.3c6
• Redesigned TCP Rate limiting for smooth control over a broad range. Use "filter action" RateLimitIn or RateLimitOut with a single parameter specifying the rate in bits per second. Can use K or M as in 100K or 1.5M bps.
• Interfaces: added Dead Gateway detection with automatic failover to alternate gateway.

• Add "Failover Locations" window to specify locations for automatic failover.
• Track connections outside of IP filtering.
• Enable "Source Aware Routing".
• Allow History->Clear to clear log windows.

Jun 1, 2005 - IPNetSentryX 1.3c5
• NKE: stream line rate limiting code when not needed.
• Trigger Table: fix bug in displaying entries of different types with the same address.
• Trigger Table: fix log message when deleting entries.

May 25, 2005 - IPNetSentryX 1.3c4
• Add "Check for Updates..." item under application menu.
• Add support for BSD interfaces not specified in the System Configuration Framework.
• Fix to restore settings when launched as a Tiger login item.

May 9, 2005 - IPNetSentryX 1.3c3
• Avoid recursive lock when starting TCP RST delay timer.
• Release lock before injecting packets.

May 6, 2005 - IPNetSentryX 1.3c2
• Fix possible panic when sequence list overflows.
• Remove seq list overflow messages from log.
• Build using Tiger GM tools.

May 3, 2005 - IPNetSentryX 1.3c1
• Rewrite NKE to support Mac OS X 10.4 (Tiger).
• Redesign Rate Limiting feature to withhold and insert Acks. Separate actions for "rate limit in" and "rate limit out".
• Fixed bug in unloading and reloading NKE consistently.
• AirPort Configuration: added "Save and Restore" checkbox to select whether to restore these AirPort settings when the application is launched or a document opened.
• Filter Table: fixed bug in matching long interface names.
• Filter Table: fixed bug uploading TCP flags with both set and reset values.
• Sentry Log: converted download and other text messages to ".plist" format.

January 18, 2005 - IPNetSentryX 1.2.05
• Preferences: reorganize and include Email settings needed by message framework.
• Ethernet Bridging: reduce MTU of bridged internal interface to match external interface if needed.

Jan 10, 2005 - IPNetSentryX 1.2.04
• Trigger table: allow editing Triggered By column.

• Trigger table: preserve last time information between application launches.
• Trigger table: remember trigger table independently from saved settings in a separate file when program quits (/Library/Application Support/Sustainable Softworks/triggerTable).
• Connection Table: age out fully closed connections sooner.

Dec 28, 2004 - IPNetSentryX 1.2.03
• Fixed LoadNKE helper that was accidently broken.
• NKE: fix possible crash when inserting TCP fragment entry.
• NKE: fix possible leak if malloc fails during AVL insert.

Dec 18, 2004 - IPNetSentryX 1.2.02
• NKE: fix possible crash if malloc fails during trigger event.
• Refactor thread to controller updates for better performance and robustness.
• Optimize check for abort in receive threads for better performance.
• Refactor thread controller classes to isolate exceptions and simplify abort and re-initialize.
• Configure NSConnections with explicit time out and queueing options.
• Remove delegate retain loops.
• Remember log drawer state.
• Show Sentry on warning when no interfaces are selected.
• Fix bug to save log text under corresponding date.
• Write a single "sentry.log" file for "ipfw" log format.

Nov 30, 2004 - IPNetSentryX 1.2.01
• Sentry Log file: use ASCII encoding when log format "ipfw" is selected.
• Do not log URL Actions.
• Fixed bug in filter action URL.
• Fixed bug in "Add Trigger" from Alert dialog.
• NKE: add OSBundleProductName and OSBundleSupportURL KEXT properties for Mac OS X Tiger.

Nov 18, 2004 - IPNetSentryX 1.2
• Validate "Save" menu explicitly when there are unsaved changes.
• Fixed bug in applying saved triggers.
• Sentry Document: fix is document edited state.
• NKE: do not bridge deleted packets.
• Release as version 1.2

Nov 12, 2004 - IPNetSentryX 1.2c7
• Trigger table: allow editing, save/restore, and apply/show to facilitate blocking a list of individual IPs.
• Alert: add trigger button to block this IP address.
• Change NKE control/server to use direct connection.
• Incorpate NKE updates and fixes from IPNetRouterX.

• SystemConfiguration - open a separate SCDynamicStoreRef for each request.
• SystemConfiguration - combine static PPP services since actual service is defined dynamically.
• Filter Action URL: borrow code from IPNetMonitorX Server Scan tool, don't open local tool windows.
• Preferences: fixed bug in Email log selections.
• Fix registration input, read key, and write key to handle international characters consistently.
• Add History menu for recent targets in built-in tools.

Aug 3, 2004 - IPNetSentryX 1.2c6
• Fix broken links in help files.
• Allow Option-Apply to clear match count and byte count.
• Show Active: report number of entries received and log any interface entries to verify configuration.
• Connection Logging: write out log every 10 minutes
• Connection Logging: update log when a connection entries time out.
• Allow up to 500 filter rules.

July 14, 2004 - IPNetSentryX 1.2c5
• Add support for Ethernet bridging.
• Added back separate window for Sentry Log.
• Address Scan: update select service popup to match target field when a scan is invoked.
• Address Scan: changed to report "Sent/Received/Lost" more consistently for TCP and UDP scans.
• Help Button and Disclosure Triangle: use 10.2.8 compatible controls.
• Registration: look for registration data in clipboard so there's no need to paste.
• Finish installation when first run is from root account.
• Try to unload NKE on first run to make sure latest version will be used.
• Improve finding PPP interfaces.

Jun 21, 2004 - IPNetSentryX 1.2c4
• Added AirPort Configuration tool.
• Try to unload NKE on first run to make sure latest version will be used.
• Improve finding PPP interfaces.
• Improved access to System Configuration Framework.
• Add Help button to "First Run" dialog and more complete error reporting when authorization is cancelled.
• History: load default targets for each tool.
• Subnet Calculator: add history support.
• NKE: fix error processing for additional rules after packet deleted.
• Logging: fixed bug when UNIX System Log format selected.
• Interfaces: add "Refresh List" button.

• Update help information.

May 24, 2004 - IPNetSentryX 1.2c3
• NKE: fix error recovery in AVL tree operations if malloc fails.
• Track PPP interface changes in System Configuration Framework.
• Preferences: select which logs to Email.
• Document Window: add log drawer in place of log window.
• Create /Library/StartupItems folder with correct permissions if needed.
• Add Help button to "First Run" dialog and more complete error reporting when authorization is cancelled.

Mar 24, 2004 - IPNetSentryX 1.2c2
• Save "Email To" field when Preferences window closes.
• Fixed bug in saving documents.
• Add "Interface ID" column under interfaces tab. Fix bug in matching system configuration changes to interface table. Allow interface name to be edited.

Mar 22, 2004 - IPNetSentryX 1.2c1
• Add "Configure As Startup Item" under application menu to save startupItemSettings.
• Configure startup item shell script and property list.
• Modified "Show Current" to load and display status from NKE previously configured by startup item.
• Restructure document state to support launching application as a startup item.
• Save Preferences in document so they can be accessed outside the context of a user login.
• Preferences: added checkbox to disable on-screen alerts.
• Save and restore trigger table as part of settings document.
• Show "status info" messages in Sentry Log window.
• Fixed bug in updating interfaces when the system configuration changes.
• Fixed bug that caused show current to not recognize duplicate entries.
• Save logs in /Library/Logs/IPNetSentryX/
• Write the Sentry log in ".plist" format as well as any user selected ".txt" form.
• Merge changes from IPNetRouterX.
• Added MacPAD.url support.

Dec 9, 2003 - IPNetSentryX 1.1
• Preferences: added "Update Logs Now" and "Email Test" buttons.
• Changed Email notification to include explicit "Date" header.
• Scrolling Views: do not scroll for updates unless bottom of view is visible.
• Release as version 1.1 that supports Panther.

Nov 24, 2003 - IPNetSentryX 1.1c8

• Restored "Authorize" action which caused subsequent actions to display incorrectly.
• Fixed to remember window size and location between sessions.
• Renamed Log Viewer to Sentry Log.

Nov 11, 2003 - IPNetSentryX 1.1c7
• Fixed crash when closing document opened at launch time under Panther.
• Fixed bug that flushed first line of log text to disk.
• Restructure to correspond with IPNetRouterX.
• Converted to use Xcode tools under Panther.

Sept 4, 2003 - IPNetSentryX 1.1c6x
• Connection log: Include ICMP type and code info.
• Connection log: show protocol ports in numeric form.

Aug 29, 2003 - IPNetSentryX 1.1c6
• Decode common C language character constants \n \r \t \b \f \0 in data content rules.
• Default configuration: added rule 2.2.1.1.9 to block WebSTAR SSL attack.
• Include byteCount in security log entries.

Aug 20, 2003 - IPNetSentryX 1.1c5
• Added connection logging.

Aug 8, 2003 - IPNetSentryX 1.1c4
• Fixed crash when "Current Filters" or "Show Active" is selected repeatedly.
• Fixed to handle exception for users that do not belong to admin group.
• Fixed to work with Panther preview (Mac OS X 10.3).
• Changed default log file path to ~/library/logs/IPNetSentryX/ .
• Security log: write a new log file each day including date as part of file name.
• Bandwidth Accounting: append new data as part of same dictionary so Bandwidth log can be opened in Apple's Property List Editor.
• Bandwidth Accounting: add preference to update Bandwidth log file after each accounting interval.

July 30, 2003 - IPNetSentryX 1.1c3
• Improved security for privileged tools.
• Refactor NKE for NAT process in IPNetRouterX.
• Remember bandwidth accounting state between launches.
• Added "authorize" action and "include authorize" property to temporarily authorize selected hosts.

July 14, 2003 - IPNetSentryX 1.0.1
• Release as version 1.0.1 .
• Change "Parent Match Count" to test against trigger table match count if

parent property = include trigger.

July 7, 2003 - IPNetSentryX 1.1c2
• Fixed "Sentry on failure" if Firewall Enabled before interfaces Applied.
• Allow independent rate limt for inbound versus outbound traffic.
• Added "keep address" action and "include address" property to detect repeated access attempts.
• Added "include state" property (connection table search) for Stateful Packet Inspection.
• Added "Parent match rate" property (number of matches/second).
• Added bandwidth accounting.
• Changed default directory for "security log" and "bandwidth log" files.

June 26, 2003 - IPNetSentryX 1.1c1
• Added TCP rate limiting (simple bandwidth management).
• Content matching: include matched text from packet in plist log record.

June 17, 2003 - IPNetSentryX 1.0
• Release as version 1.0 .

June 13, 2003 - IPNetSentryX 1.0c2
• Fixed initialization bug in connection state table that caused packets to be deleted.
• Remember trigger expiration when NKE is reloaded.

June 11, 2003 - IPNetSentryX 1.0c1
• Include QuickStart settings and QuickStart ReadMe.
• View help in default web browser.
• Added properties for "Date and time", "Idle seconds", and "MAC Address".
• Fixed offset bug in "Reject" action.
• Fixed display of local image for Drop Connection.
• Interfaces: update IP addresses when IPv4 configuration changes.
• Work around bug in PPP frame header info.
• Preserve matchCount and byteCount when settings are Applied.
• Preserve expandedState after "Show Active".
• Triggered tab view: show trigger expire time for each entry and reflect changes immediately.
• Optimize filter update process to ignore subnodes if parent hasn't changed.
• Optimize trigger update process to cache "leastRecent" and "mostRecent" entries.
  Skip tree search if no timeouts or updates based on cached values.
  Check for trigger updates each second.
• Drag & Drop: show dropped items as selected.

May 28, 2003 - IPNetSentryX 1.0b10
• Triggered Tab View: show rule # and match count.

• Triggered Tab View: added Lookup button.
• Triggered Address Table: fixed same time bug that prevented entries from being deleted correctly.
• Log: show sub actions (Alert, Email,...) and don't log the same event twice.
• Alert: change window level to "NSStatusWindow" to appear in front of others.
• Log kernel event messages for PROTO_ATTAHCED and IF_DETACHED.
• Address Scan: re-use the same window.
• Update stats correctly after "Show Active".

May 22, 2003 - IPNetSentryX 1.0b9
• Added "Firewall Documents Window" help section.
• Add Triggered address tab view to examine and delete triggered IP addresses.
• Make triggered address expiration time adjustable.
• Add Test button to launch web based firewall test URL.
• Include more information in Security Alert panel.
• Added "Show Log" button to Security Alert panel.
• Attempt to open other URL types as action parameters of firewall rules.
• Removed WhoIs tool, launch IPNetMonitor tool instead.
• Enable and select newly created rules.
• Send multiple updates as separate UDP records.
• Show statistics with corresponding rule when interface list is included as part of configuration.
• Correct delta statistics when counts are reset.
• Convert trigger table to use AVL tree, allow up to 2000 entries.
• Fix crashing bug when application is launched from a firewall enabled document.
• Do not mark document as changed when edited fields keep their previous value.

May 5, 2003 - IPNetSentryX 1.0b8
• Added tab view for selecting firewall interfaces.
• Update document change count to inform user when there are unsaved changes.
• Added "Reject" filter action to explicitly refuse connection requests (send RST).
• Update default configuration to Reject "AUTH" port 113 connection requests used by some mail servers.
• Add "Don't Log" action to allow making any leaf action silent.
• Wait for KEV_DL_PROTO_ATTACHED to insert NKE when PPP connects.
• Remove any stale attachment before inserting NKE.
• Update AddressScan, Lookup, and TCPDump tools from latest IPNetMonitorX.

April 17, 2003 - IPNetSentryX 1.0b7

• Use 64-bit integers for matchCount and byteCount.
• Subtract frame header length from byteCount of outbound packets.
• Expand default configuration to include rules for protecting common services.
• Use MoreSCF to enumerate available network devices and names.
• Monitor kernel events to insert NKE when a new interface appears (PPP connects for example).
• Updated "Getting Started" documentation.

April 7, 2003 - IPNetSentryX 1.0b6
• Fixed setting firewall enabled state when a document is opened.
• Save and restore which rules are expanded in filter documents.
• Save and restore parameter popup state in filter documents.

April 2, 2003 - IPNetSentryX 1.0b5
• Fixed possible kernel panics:
  Protect connect to NKE to avoid multiple outstanding requests.
  Protect socket buffer calls, and inserting/removing NKE.
  Use synchronous Distributed Object methods to setup NKE.
  Use correct buffer size (MCLGET) for NKE to client messages.
• Use OSAddAtomic() for shared counters.
• Limit SentryOn to confirm client is listening to once every 2.5 seconds.
• Parameter column, do not allow editing rule statistics.
• Show change from last update for matchCount and byteCount.

March 17, 2003 - IPNetSentryX 1.0b4
• Protect dynamic tables in NKE from pre-emption to fix crashing bug.
• Update node numbers consistently before downloading filter rules.
• Expand default configuration to include ICMP logging, ping flood protection, block source route, and block additional attack signatures.
• Add "Current Filters" tool to open a filter window and upload the kernel filter table.

March 10, 2003 - IPNetSentryX 1.0b3
• Fix idle timer to skip disabled entries (so Address Scan tool doesn't appear unless server monitoring is enabled).
• Hide disclosure triangle for entries with no children (not expandable).
• Add Sibling/Child button to toggle "New Sibling" versus "New Child" for entries that do not have a disclosure triangle. Pressing this button (keyboard shortcut <CR>) will expand or collapse the selected entry if any. Can aslo use this to control where data is pasted (as a sibling or child).
• Restore descriptive text of Property Value when showing active configuration.
• Fixed parameter text when showing active configuration.
• Include description of ICMP type and code in text logging format.
• Extend public beta period.

February 17, 2003 - IPNetSentryX 1.0b2
• fixed "idleTimeOfParent" and URL notification.
• Address Scan: re-use the same window.

February 14, 2003 - IPNetSentryX 1.0b1
First publicly posted beta test version of IPNetSentryX.

This beta version demonstrates all of the core features of IPNetSentryX but has not been widely tested by external users. As such, you should view it with some caution. While it has proven stable in our own testing, bugs in network kernel code can result in a kernel panic forcing you to restart your machine.

Known Limitations:

Drag-and-drop between firewall rules is not fully debugged yet. Use copy-and-paste instead.

[End of Release Notes]