



VERSION 2.0

RELEASE NOTES

COPYRIGHT NOTICE

Copyright © 2006-2008 Netronome Systems, Inc.
All Rights Reserved.

No part of this document or documentation accompanying this Product may be reproduced in any form or by any means or used to make any derivative work by any means including but not limited to by translation, transformation or adaptation without permission from Netronome Systems, Inc., as stipulated by the United States Copyright Act of 1976. Contents are subject to change without prior notice.

NO WARRANTY

The technical documentation is being delivered to you **AS-IS** and Netronome Systems makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. The documentation may include technical or other inaccuracies or typographical errors. Netronome reserves the right to make changes without prior notice.

LIABILITY

Regardless of the form of any claim or action, Netronome's total liability to any user of this documentation and the SSL Inspector Appliance, for all occurrences combined, for claims, costs, damages or liability based on any cause whatsoever and arising from or in connection with this documentation shall not exceed the purchase price (without interest) paid by such user.

IN NO EVENT SHALL NETRONOME OR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE DOCUMENTATION OR THE SSL INSPECTOR APPLIANCE, BE LIABLE FOR ANY LOSS OF DATA, LOSS OF PROFITS OR LOSS OF USE OF THE DOCUMENTATION OR LOSS OF USE OF THE SSL INSPECTOR APPLIANCE OR FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, PUNITIVE, MULTIPLE OR OTHER DAMAGES, ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR THE USE OF THE SSL INSPECTOR APPLIANCE EVEN IF NETRONOME HAS BEEN MADE AWARE OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL NETRONOME OR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE DOCUMENTATION OR THE SSL INSPECTOR APPLIANCE BE LIABLE TO ANYONE FOR ANY CLAIMS, COSTS, DAMAGES OR LIABILITIES CAUSED BY IMPROPER USE OF THE DOCUMENTATION OR THE SSL INSPECTOR APPLIANCE OR USE WHERE ANY PARTY HAS SUBSTITUTED PROCEDURES NOT SPECIFIED BY NETRONOME.

1. New Features

- New modes for SSL inspection were added. Passive mode decrypt allows for decrypt on SSL traffic received from a tap/SPAN port. IPS fail-to-network mode was added to support a different cable configuration that will allow bypass of the IPS device in case of a failure.
- Advanced failure mode options to provide automatic response and controlled degradation of performance in case of software, appliance and/or network failure.
- Configurable email alert system to notify administrators of potential problems and send periodic status updates.
- Ability to bypass the attached appliance completely in filtering/IPS mode in a fail-to-appliance configuration.
- Increased maximum number of concurrent SSL and non-SSL flows.
- Changed the no-activity timeout to be one hour for inspected SSL flows and infinite for non-SSL and non-inspected flows.
- The SSL session log, system statistics and audit log files can now be exported for audit, backup or data mining purposes.
- Device configuration export/import features can now be controlled from the web interface in addition to the command-line interface.
- IPS resets for plaintext flows generate TCP RST packets in both directions in the original SSL flow.

2. Issues Resolved

- SSL flows in fragmented TCP were stalling because of an issue in the decrypt/re-encrypt engine.
- SSL flows with expired certificates were erroneously being logged in the SSL session log as having a valid certificate.
- The TCP three-way handshake is now handled differently to mitigate excessive SYN floods. Precious SSL decrypt/re-encrypt engine resources are not allocated until required.
- The chassis intrusion detection shown on the front panel can now be cleared using the web interface.
- Administrators often forget to apply changes to the active policy. A warning message was added that persists until the administrator applies the policy changes.
- In some cases the decrypt/re-encrypt engine did not limit the number of bytes used to calculate the SSL record MAC, with the following error as result: "SSL record MAC could not be verified".
- The decrypt/re-encrypt engine now directs TCP flows to send packet retransmits on packet boundaries previously seen in the flow. This was done to solve re-encrypt issues with retransmitted packets.
- ARP packets were being sent to the IPS device when a bypass Traffic Diversion Policy was activated.
- Various changes were made to the way the audit user interacts with the web interface. One example is that the audit user was not able to view the link status.
- Undecryptable SSL flows were not consulting the SSL Inspection Policy and consequently not being logged in the SSL session log.
- When NTP servers were added, deleted or modified while NTP was enabled, or when NTP was enabled after being disabled, the SSL Inspector Appliance previously adjusted its real time clock over a long time period. The SSL Inspector Appliance's real time clock will now jump to the time indicated by the configured NTP server(s).
- The DSCP value was not set when the Traffic Diversion Policy was configured to mirror traffic. UDP traffic was also not being mirrored.
- The key ID used for known keys in the web interface was displayed differently on the policy and PKI pages.
- Some IPS devices reported invalid TCP traffic in the generated plaintext stream. This was because of a missing TCP ACK flag on the last TCP FIN.

- A certificate without a common name could be imported as a known-key certificate and used in the SSL Inspection Policy. The known-key import process now prevents this.
- The SSL Inspector Appliance unexpectedly dropped flows in a HA (high-availability) scenario during the cut-back from the backup device to the original device.
- The management system would constantly reboot the SSL Inspector Appliance in the case of a NPU (network processor) failure. Reboots are now limited.
- Administrators are now logged out if their accounts are deleted (using another web interface session or using a command line interface command).
- Some TCP flows were erroneously being classified as SSL with a subsequent false re-encrypt failure.
- The reliability of the NPU health checking mechanism has been improved. This will avoid unnecessarily triggering recovery actions (e.g. rebooting the platform).
- The SSL Inspection Policy sort order was wrong. This is important because rules are auto-sorted.
- The SSL handshake on inspected flows was still being sent to the IPS device, and the handshake packets had sequence numbers in different TCP sequence spaces. The SSL handshake is no longer sent to the IPS device.
- SSL flows that were rejected by the SSL Inspection Policy because of invalid certificates were not properly terminated with a TCP RST.
- The graph viewer would occasionally display the time in the old time zone during a time zone change.
- The clock display in the "Date and Time" user interface did not change when a month boundary was crossed.
- False "session verification failure" errors were logged when the SSL Inspection Policy was set to cut through all flows.
- Mechanisms were added to detect and recover from database corruption.
- X.509 certificates with Extended Validation (EV) were not handled properly. Certificates with EV are now re-signed by removing the EV attributes after validation.
- Logic was added to detect SSL flows that violate the SSL/TLS specifications. These flows are now subject to the "Undecryptable SSL Handling" parameter in the SSL Inspection Policy.

3. Known Issues

- If the SSL Inspector Appliance is used in network configurations that use asymmetric routing, one direction of each TCP connection might end up not being routed through the appliance. The SSL Inspector Appliance will reject all TCP connections that were not properly established.
- The SSL Inspector Appliance does not support the transparent TCP session hijacking feature of some IPS devices. This feature allows IPS devices to display messages to end users to indicate that content has been filtered or quarantined. The IPS devices normally transparently terminate the TCP session and inject HTML text or an HTTP redirect instruction. The SSL Inspector will reject the flow, thereby immediately terminating the TCP session and preventing the HTML message or HTTP redirect from reaching the end user.
- The SSL 2.0 and TLS 1.1 protocols are not yet supported. The behavior of the SSL Inspector Appliance when these protocol versions are detected is governed by the "Undecryptable SSL Handling" parameter in the SSL Inspection Policy.
- The web interface will require policy re-activation whenever the active policy has been modified. This applies even if the only change to the active policy was to add comments to rules.
- Recent implementations of SSL/TLS add extensions as described in RFC4366. The SSLIA is not compatible with the session resumption extension described in RFC4507.
- ARP packets are not mirrored to the IDS device when the Traffic Diversion Policy is configured to mirror traffic.
- TCP RST and ICMP packets generated by the IDS device are ignored and not propagated to the SSL client and the SSL server. Note that TCP RST packets are handled correctly in IPS modes.
- The SSL Inspector Appliance can experience unusual delay when a large number of connections close simultaneously. This is unlikely to happen, but certain test equipment can reproduce the scenario.
- Pressing the manual bypass button on the front panel will not result in a log entry or alert.
- User passwords are not included in the file generated during an export.
- The 'nsexport' utility will, by default, not include any PKI data. This implies that all root CA certificates added by the customer will not be exported by default. The solution is to explicitly include PKI data with the "--include" option.

4. Technical Support

To obtain additional information or to provide feedback, please email support@netronome.com or contact the nearest Netronome Systems technical support representative.

Visit <http://support.netronome.com> to download the latest documentation and software, access the knowledge base, or log a support ticket.