



VERSION 2.3

RELEASE NOTES

1. New Features and Optimizations

- Enhanced diagnostics capabilities with more debug information.
- The SSL inspection engine now supports stateless TLS session re-use (RFC5077), typically used by Firefox 3.6 and some large server deployments, such as www.gmail.com.
- The inspection policy was extended to allow for matches on source IP/mask, destination IP/mask and destination TCP port.
- Added a screen to the frontpanel that displays the current network interface status. This is especially useful for fiber deployments.
- Added more navigation buttons and more representative names for each certificate to the Trusted CA Certificates WebUI page.
- The list of trusted CA certificates was updated to include the latest root CA certificates and widely used intermediate CA certificates.
- Added various packet error checks in the packet processing engine to prevent invalid packets from reaching the SSL inspection engine.
- The SSL detection logic was enhanced to reduce the number of false positives.

2. Issues Resolved

- Packets differing only in VLAN tag were corrupting the packet processing engine in the SSL Inspector Appliance. This only occurred in IDS Passive mode. The VLAN tag now forms part of the search key that maps packets to unique flows.
- If the network TAP/SPAN port feeding a SSL Inspector Appliance in IDS Passive mode is dropping packets it will result in gaps in the reassembled TCP streams. The TCP streams will eventually time out and result in warning messages in the dataplane log file.
- The CA certificate generated by the SSL Inspector Appliance did not have the correct attribute to qualify as a CA certificate.
- The database of previously seen server certificates is now limited to 20,000 entries.
- Fixed a bug in the network interface status detection logic.
- Importing a known private key that was already in the PKI store corrupted the policies using the key.
- Flows on which SSL was not detected were not properly diverted to the fast path of the packet processing engine.
- IDS Passive mode load balancing now also load-balances non-SSL flows.
- Fixed mirroring of non-inspected SSL flows in IDS inline mode.
- Enhanced handling of IP fragments, including advanced error checks.
- Non self-signed certificates corrupted the Trusted Certificates store during import.
- Fixed issue where having a non accessible DNS server configured in the network configuration prevented the WebUI from operating.
- Fixed issue with `nsimport` utility that prevented importing certificates and keys in PEM format.

3. Known Issues

- Due to an issue with protection on exported configurations in version 2.0 of the SSL Inspector Appliance it is impossible to import PKI information from configurations exported from version 2.0. Do not select the PKI option when importing the configuration. Note that this is **not** a problem when importing configurations exported from version 2.1 onwards.
- The web interface log search facility will, in some cases, not search all the pages in the log viewer. A work-around is to jump to the end of the log file (with “Last” button) before changing the search field.
- Importing an exported configuration file that contains policy information will not automatically activate the previously active policy.
- The RC4-ADH cipher-suite is not on the list of supported anonymous Diffie-Hellman cipher-suites.
- Invalid retransmitted TCP SYN packets might, in some cases, cause a failure on existing flows. This would be considered a DOS (denial-of-service) attack because normal TCP endpoint stacks would not generate the packets that cause the failure.
- Two certificates with the same common name (in X.509 subject) cannot both be added to the “Known Server Keys” store.
- 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 ignore 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 protocol is not supported. The behavior of the SSL Inspector Appliance when this protocol version is 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.
- 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.
- If Ctrl-C is pressed while the *nsdiag* utility is busy, it might, on rare occasions, indefinitely pause the Database Commit Daemon. If *nsdiag* has completed and the last log entry in the Database Commit Daemon log is still "Pause queue processing" and not "Resume queue processing", the following command can be issued to restart the process: `nsservice nsdbcmdd restart`

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.

COPYRIGHT NOTICE

Copyright © 2006-2010 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.

Product Code: 080-00002-006