Sourcefire SSL Appliance Release Notes

Version 3.6.3

September 5, 2013

These release notes are valid for Version 3.6.3 of the following platforms of the SSL appliance:

- SSL1500
- SSL2000
- SSL8200

Even if you are familiar with the update process, make sure you thoroughly read and understand the release notes, which describe supported platforms, new features and functionality, known and resolved issues, and product and web browser compatibility. They also contain detailed information on prerequisites, warnings, and specific installation and uninstallation instructions.

For more information, see the following sections:

Important Update and Compatibility Notes

The following sections list important points you must keep in mind before you begin the update process, as well as any possible consequences or compatibility issues you may encounter during or after the update process:

Before You Begin

Before you begin the update process for Version 3.6.3, you should keep the following important points in mind:

- Sourcefire **strongly** recommends that you back up event and configuration data to a local computer before you perform the update; this data is **not** backed up as part of the update process.

  For information on the backup feature for your appliance, see the *Sourcefire SSL Appliance Administration and Deployment Guide*.
- All SSL appliances running earlier software versions **must** be upgraded to the software version described in these release notes. If an item below only applies to the SSL1500, SSL2000, or SSL8200, this is clearly indicated. Otherwise, all items apply to all appliances.
- If you need to return your appliance to a previous release of the SSL appliance for any reason, contact Sourcefire Support for more information.

New Features and Functionality

The following features and functionality have been added in Version 3.6.3:

- Added support for ECDHE-ECDSA SSL/TLS cipher-suites, which includes support for ECC-DSA certificates.
- Added support for Google ChannelID TLS extension, which allows the Chrome browser to properly connect to Google servers through the SSL Visibility appliance.
- Added CLI tool to collect diagnostics, which was previously only possible via the GUI.
- Version and S/N information is now displayed on CLI as well as on the front panel LCD.
- Recovery partition version information added to GUI.
- Limit on concurrent connections on the SV3800 increased from 300,000 to 400,000.

The following features and functionality were added in Version 3.6:

- Support for inspecting TLS 1.2 traffic
- Better handling of TCP RST packets

- Cache layer2 information per direction for the purpose of building ACK packets and plaintext packets
- Hide some of the debug counters
- Added more debug counters to NFP
- Option to configure a second remote syslog server
- Enhanced login dialog, including version checking
- Updated external CA list
- Monitor platform, then log warnings when certain sensors/values go above/below preset limits
- Ability to trigger memtest from grub
- Option to enable automatic recovery from HA failure
- SNMP configuration, including editable fields
- Switched to using latest Geryon BIOS/BMC/Config
- Support for TACACS+/ACS remote authentication and accounting
- Support for large CN and IP lists
- Added audit entry for CA export
- Added paging to all lists
- Mechanism to clear statistics and counters
- System log entry for sessions rejected because of client certificates
- Filtering on in-memory SSL session log
- Support for SSL in fragmented TCP
- Save management network configuration when installing a system update
- Display BIOS and BMC versions on user interface

Issues Resolved

The following issues were resolved in Version 3.6.3:

- Fixed mechanism that applies policy to IP fragments.
- Fixed case sensitivity of CN-list matching.
- Fixed bug in packet header cloning, which would have affected ACK generation.
- Fixed bug in passive mode reassembly logic, which caused “stalls” on sessions with large certificates.
- Only cache SSL sessions with useful information (i.e. do not cache non-inspected session if certificate is not valid).
- Fixed potential segfault in IP fragment handler.
- Fixed TCP stalls for cut-through rules in inline modes.
- Capture generated ACKs in debug PCAPs.
- Added dropbox.com to list of unsupported sites.
- Fixed potential segfault in platform status API.

- Cache SSL sessions with cut-through action (to get access to CN for reused sessions) – unavailable previously.
- Fixed generation of ACKs in decrypted sessions (use received acknum vs sent acknum).
- Fixed retransmit logic on some block-cipher cipher-suites.
- Fixed user database authentication issues.
- Fixed issue with editing rules where the X.509 subject was not unique.
- Fixed user interface certificate import mechanism.
- Fixed internal PKI object corruption, which could have caused misclassification of flows and UI errors when viewing SSL sessions.
- Fixed handling of fragments in passive mode.
- Fixed user interface issue where custom PKI lists could not be managed.
- Fixed corruption of persistent certificate cache.
- Fixed potential issue in the timeout handler, which would have prematurely ended some SSL sessions.
- Fixed issue with premature overload detection on SV3800.
- Decrypted SSL sessions that run into an error will now be terminated, even if the SSL intercept mechanism did not modify any of the payload in the original stream. This fixes an issue where encrypted payload was sent to the attached appliance after an error.
- Reduced verbosity of logs on serial console.
- Removed invalid and/or untrusted external CA certificates from distribution.
- All user IDs are now case insensitive, and will be displayed in lower case even if entered in upper case.
- Fixed handling of long DN strings, to prevent potential segfault.
- Removed untrusted and non-public external CA certificates.
- Added EC-signed external CA certificates (previously not included due to lack of EC key support).
- Fixed an issue with enforcement of concurrent sessions limit.
- Replaced CPU overload system log entries with an internal CPU overload counter.
- Implicitly trust all known certificates, i.e. certificates with keys imported into the PKI store on the appliance.
- Fixed handling of no-payload TCP packets, which caused various queue processing timeout issues.CP packets, which caused various queue processing timeout issues.

The following issues were resolved in Version 3.6:

- Does not crash during diagnostics collection, due to remote syslog configuration.
- Large SSL certificate chains when rule=CUT are handled properly.
- Fixed internal CA CSR (basic constraints, key-usage).
- Fixed Passive-Tap HA mode operation.

- Supports auto-update of BIOS/BMC on Pegasus chassis.
- Fixed handling of retransmits to resolve "internal errors".
- Does not bypass the ruleset for undecryptable sessions.
- Less stringent SSLv2 ClientHello checks to fix SSL detection.
- Fixes issues when IE8 was used to connect to appliance UI.
- Includes qdesc information in diagnostics.
- Fixes potential crash in control daemon, related to firmware version checking.
- Fixes retries on platform interface calls.
- Fixes issues with TCP windows and unique IP IDs.
- Added timeouts and rate-limiting on early ACKs.
- Disables early ACKs as soon as a TCP RST is seen on the wire.
- Fixes ruleset issue when session has invalid certificate handle.
- Fixes lockup in DN parsing.
- Fixes sslcli unfail option.
- Does not allow cancel of update if already canceled.
- Retries UI call on role expiry.
- Allows cancel on rescue updates.
- Fixes to TCP inline library gap detection (to resolve stalls on large downloads).
- Turns off GRE/MPLS support (unsupported in host code).
- Fixes password check wordlist (uses correct wordlist package).
- Fixes issues in end-of-flow handling.
- Fixes handling of TCP window updates advertised in TCP ACK packets.

Updating Existing Appliances and Software Sensors

There are three methods for updating your SSL appliance from Version 3.6.x to 3.6.3. You can use a patch, which requires downloading and updating two files on the SSL appliance, or you can use an image on a USB stick, which requires building a bootable USB stick.

The following sections help you prepare for and install the Version 3.6.3 update on your existing SSL appliances:

- Planning for the Update on page 6
- Updating the SSL Appliance Using a Patch on page 6
- Updating the SSL Appliance using the System Update Mechanism on page 7
- Updating the SSL Appliance Using an Image on a USB Stick on page 8

Planning for the Update

This section outlines how to plan for and perform the Version 3.6.3 update for the SSL appliance.

To update your SSL appliances:

1. **Read these release notes.**

   Even if you are familiar with the update process, make sure you thoroughly read and understand the release notes, which describe supported platforms, new features and functionality, known and resolved issues, and product and web browser compatibility. They also contain detailed information on prerequisites, warnings, and specific installation and uninstallation instructions.

2. **Make sure your appliance is running the correct version of the SSL appliance.**

   To use the patch mechanism to update to Version 3.6.3, your appliance must be running at least Version 3.6.0. If you are running an earlier version, you can obtain updates from the Sourcefire Support Site.

   TIP! If you do not want to retain configuration or policy data, you can update with the system update mechanism to re-image the SSL appliance.

3. **Back up current event and configuration data to an external location.**

   Sourcefire **strongly** recommends that you back up current event and configuration data to an external location. This data is **not** backed up as part of the update process.

   For more information on the backup feature, see the *Sourcefire SSL Appliance Administration and Deployment Guide*.

Updating the SSL Appliance Using a Patch

Updating the SSL appliance with a patch is a two-step process. You apply the patch to a SSL appliance running Version 3.6.x, and then after confirming that the appliance is running Version 3.6.3 you must update the system rescue image to Version 3.6.3.

The following section describes how to update the SSL appliance using the patch.

To update the SSL appliance using a patch:

1. Read these release notes and complete any required pre-update tasks.
2. Download the following patch files from the Sourcefire Support Site to a local device accessible by your SSL appliance:

   ```
   sslng-3.6.3-841-sf.patch
   sslng-3.6.3-841-sf.nru
   ```

   IMPORTANT! Download the update directly from the Sourcefire Support Site. If you transfer an update file by email, it may become corrupted.

3. On the system tab (which may be labeled with the name of the system) on the user interface of your SSL appliance, click **Update**, and select **Choose File** from the dropdown menu.

   A window opens to browse for the update file.

4. Locate and select the following file from the downloaded patch files, and click **OK**:

   ```
   sslng-3.6.3-841-sf.patch
   ```

5. When prompted, click **Reboot**. The update can take three to five minutes to complete.

   WARNING! This step may perform firmware updates. Do not reset the system while firmware updates are taking place or the system may become unusable.

6. After reboot, log into the appliance and confirm that the appliance is running Version 3.6.3-841.

   After confirming that Version 3.6.3-841 is installed and running correctly, update the rescue image on the SSL appliance to Version 3.6.3-841.

7. On the system tab (which may be labeled with the name of the system) on the user interface of your SSL appliance, click **Update**, and select **Choose File** from the dropdown menu.

   A window opens to browse for the update file.

8. Locate and select the following file from the downloaded patch files, and click **OK**:

   ```
   sslng-3.6.3-841-sf.nru
   ```

9. When prompted, click **Reboot**, and wait for the update to complete. This may take several minutes.

   WARNING! This step may perform firmware updates. Do not reset the system while firmware updates are taking place or the system may become unusable.

Updating the SSL Appliance using the System Update Mechanism

The system update mechanism will retain the system settings, including the management IP address, but will not retain configuration or policy data. You will access the SSL appliance after the update, but will need to go through the bootstrap process.

To update the appliance using the system update mechanism:

1. Download the following ISO file:
   `sslng-3.6.3-841-sf.nsu`
2. On the system tab (which may be labeled with the name of the system) on the user interface of your SSL appliance, click **Update**, and select **Choose File** from the dropdown menu.

   A window opens to browse for the update file.
3. When prompted, click **Reboot**, and wait for the update to complete.

   This process can take several minutes, and may reboot more than once.

   WARNING! This step may perform firmware updates. Do not reset the system while firmware updates are taking place or the system may become unusable.
4. Connect to the appliance using your assigned IP address. If you are using DHCP, the IP address will display on the LCD Panel. If you are using a static IP address you will need to restore the static IP address using the front panel of the appliance.
5. Confirm that the the appliance is running Version 3.6.3-841.
6. Complete the bootstrap process using the WebUI.

Updating the SSL Appliance Using an Image on a USB Stick

The following section describes how to update the SSL appliance using a bootable USB stick.

You can use the Linux client or download a tool for Windows (for example, Launchpad Imagewriter) to build a bootable USB stick.

To update the appliance using a bootable USB stick:

1. Download the following ISO file:
   `sslng-3.6.3-841-sf.iso`
2. Build a bootable USB stick from the ISO file using Linux or Windows.
3. Prepare console (serial or VGA) access to the SSL appliance.
4. Plug the USB stick you created into a USB port on the SSL appliance, and reboot the appliance.

5. When the GRUB menu appears, select **Manufacturing DOM install** and press Enter.

   TIP! If you are using an SSL Appliance 1500, and the GRUB menu does not appear, reboot the appliance and press F11 during bootup, select the USB stick option from the bootable devices menu, and press Enter.

   The appliance will shut down to reboot after the process completes.

6. When the system shuts down to reboot, remove the USB stick.

7. When the GRUB menu appears, select **Factory install** and press Enter.

   This process can take several minutes, and may reboot more than once.

   WARNING! This step may perform firmware updates. Do not reset the system while firmware updates are taking place or the system may become unusable.

8. Connect to the appliance using your assigned IP address. If you are using DHCP, the IP address will display on the LCD Panel. If you are using a static IP address you will need to restore the static IP address using the front panel of the appliance. Complete the bootstrap process on the WebUI.

Uninstalling the Update

There is no mechanism to uninstall the update. If you need to remove the update from your SSL appliance, you can restore the appliance to its original factory settings. Note that all stored data, logs, configurations, and any other information will be erased during the restore procedure.

If you need to restore your SSL appliance to its original factory settings, call Sourcefire Support for assistance.

Known Issues

The following is a list of known issues:

- Ethernet jumbo frames are not supported.
- The SSL appliance has not yet been optimized for optimal throughput.
- Some SSL sessions may fail with invalid SSL MAC calculations. This is usually an indication that packets on the wire are corrupt, or have been tampered with.
- Restoring a policy that contains active segments does not always activate the segments. The workaround is to manually activate the segments.
- Some SSL servers use SSL certificates with invalid subject distinguished names. Those subjects cannot be parsed by the SSL engine for the purpose of making a policy decision.

- PKI objects (certificates or keys) can be removed even if they are still referenced by the active policy. The SSL engine does not fail if the policy is invalid, but all rules using invalid or missing PKI objects are ignored.
- If more than one administrator is making changes to the SSL appliance configuration, they will have to log out and log in again before changes made by the other person are reflected in the user interface.
- A segment configured to use any of the Active-Inline (AI) modes rejects, under load, some of the SSL sessions because of packet feedback timeouts. This means that decrypted packets sent to the attached device (such as IPS) do not return in time to complete the feedback loop required to trigger a re-encrypt of the original packets.
- A TCP FIN/FIN-ACK/ACK sequence is generated at the end of each decrypted SSL session. The three packets in this sequence may arrive at the attached device (e.g. IDS) out of sequence. This should not pose problems for TCP reassembly devices.
- Updates to the system log are only reflected on the last page, and only after pressing the **Last** button.
- Internal CA certificates are not automatically checked for expiration. As a workaround, periodically check the certificates on the user interface.
- Only network interfaces used by active segments will change color on the user interface dashboard, based on the status of the interface.
- SSL session logs may capture false positives, which are flows that look like SSL but are not SSL. Each session log entry also contains a flag that indicates whether the session has been confirmed as valid SSL, specifically whether the policy decision has been applied to the session. This flag does not appear on the user interface, but SSL session log post-processing tools can use this flag to filter out all false positives.
- When the SSL appliance recovers from an overload condition it may flag some SSL sessions with the `Invalid cryptographic response` error code.

Web Browser Compatibility

Version 3.6.3 of the web interface for the SSL appliance is compatible with the following browsers:

- Firefox 11.x
- Chrome 18.x
- Microsoft Internet Explorer 8.x and 9.x

For Assistance

If you have any questions or require assistance with the Sourcefire SSL Appliance, please contact Sourcefire Support:

- Visit the Sourcefire Support Site at https://support.sourcefire.com/.
- Email Sourcefire Support at support@sourcefire.com.
- Call Sourcefire Support at 410.423.1901 or 1.800.917.4134.

Thank you for using Sourcefire products.

Copyright Notice

No Warranty

The technical documentation is being delivered to you AS-IS and Netronome Systems makes no warranty at 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.

Third Party Acknowledgements

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).