WebApp Secure 5.1.3-3

(formerly Junos WebApp Secure (JWAS) or Mykonos)

Release Notes: (November 19, 2013)

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

November, 2013

Contents

For additional information about WebApp Secure, please refer to the *WebApp Secure Administrator Guide and WebApp Secure Developer Guide.*

Synopsis

5.1.3-3 Maintenance release contains minor features, improvements and bug fixes with a notable feature addition of improved support of customer sites fronted by Akamai CDN, sometimes referred to as Dynamic Site Accelerator (DSA). In addition to these enhancements and bug fixes, the documentation has been reworked to better match unified Juniper documentation format.

Please **note** that the name "Junos" is being dropped from "Junos WebApp Secure (JWAS)". The product name is now “WebApp Secure” and that will be used throughout all User Interface and Documentation.

Installing and Deploying WebApp Secure

The installation procedure for WebApp Secure remains the same. As soon as the update is available, it will be downloaded by the system automatically if the system is connected to the WebApp Secure Support System. After the upgrade, **system requires a reboot** since the Linux Kernel version has changed from 2.6.32-279.5.1 to 2.6.32-358.18.1.

CDN (Akamai) Support:

- The problem we are trying to solve with this feature, in a nutshell, is making WebApp Secure work with Akamai CDN/DSA (Dynamic Site Accelerator) with minimal modifications. Dynamic Site Accelerator is an Akamai product designed for mostly-dynamic websites and it functions as a distributed reverse proxy between end-users and WebApp Secure and can be configured to provide caching features. This feature allows for the proper identification of the IP address of the end-user visiting the protected site via Akamai CDN/DSA.
- The main problems to solve are:
    - Getting the actual IP address of the client/browser since otherwise WebApp Secure will only get Akamai’s IP Address
    - Getting control over the caching features of DSA in such a way as to allow our tar traps and tracking code to work, else those WebApp Secure specific content may get cached by Akamai which would reduce WebApp Secure’s effectiveness.
- To get the actual IP address we use the “True-Client-IP Header” that Akamai sends, this header can be configured by customers as described later.
- For getting control over caching feature so that WebApp Secure functions correctly, WebApp Secure uses “Zero-TTL” feature of Akamai for WebApp Secure specific contents. This is an internal change and customer site is not impacted.

Enhancements

Management Graphical Interface

- Incidents/Attackers: unified way of referencing attackers by their local name vs. current mixed global (Spotlight) and local naming in various tables
- Responses: added Deactivate All option to the Responses area vs. disabling them one by one
- System status: added Routing table, Services and Backend server health status pages
- Reporting: added time zone option to both on-demand and scheduled reports
- Applications Setup/Configuration: added New Application wizard which walks the user through the necessary steps and important options of setting up an application in a wizard-like format; modified the

way context of the configuration (application vs. global) is being accessed – each application is now represented as a node in the navigation tree giving user clear view into which settings they are modifying

- Configuration: converted some setting values to better match their purpose vs. utilizing their indexes in configuration ("Allow" vs. "1"); groups processors by their category to better match their purpose
- Authentication: Added warning message about impending login block: when the WebApp Secure Admin fails to login multiple times then admin is warned about their temporary suspension of their access
- Preferences: Added "Prompt Level" parameter to control whether the textual help around the settings is displayed or not, the default is to show textual help
- Inline Documentation: White list exclusions clarified and one (non-working item) removed from UI for Security Engine Whitelists. The white list exclusion allows for
    - Trusted IP Addresses: The IP addresses in this list will not trigger incidents.

Additional Improvements:

- Database Cleanup Service is now "Enabled" by default.
- Added stricter validation around several parameters to disallow mistakenly entered values
- Replaced localhost with an actual system's hostname in syslogs
- Added proxy exclusion list parameter (engine.proxy.exclusions) to allow certain known types of resources, like images, or zip files to be skipped by the security processing; since WebApp Secure injects it's trap into HTML content, processing binary data can have impact on system load and reduce processing throughput capacity of the device and/or add additional latency
- Backend health checks are now configurable by the customer vs. being static 60 seconds
- Log File Rotation is now configurable
- Status of Spotlight enabled/disabled is now sent to support site with the nightly check-ins
- Timeout from WebApp Secure to backend server can now be set, the current default is 60 seconds.

Bug Fixes: Several bugs were fixed. A few important ones are listed below.

- HTTP POST content type other than multi-part and url-encoded not supported
- Errors when fingerprint submissions were empty
- Threat and Skill for profiles are not properly updated if the attacker's profiles come from Spotlight and then start to hack locally
- ETAG processor on certain pages consumes all cpu cycles and takes down Security Engine
- Search results were not showing up with large number (>200) of attacker's profiles and incidents
- Configuration UI does not authenticate RADIUS servers correctly
- No way for admin to unlock an account after 6 failed login attempts, which now can be done with the CLI
- Alerts page with incorrect shift values was being saved
- Admin was unable to navigate to attacker's profile if its name is saved with 'Space' character
- Out of Memory errors when generating reports with large amounts of db content
- Unable to view Incident details in UI if request or response are not enabled for recording, this is fixed now. Incident details will be available even if the requests or response are not being recorded.
- All the attackers' profiles get displayed on sorting by pages on Spotlight page, it now shows only the relevant attackers profiles.

- WebApp Secure does not recompress compressed responses after they pass through security engine

Known Issues and Limitations with 5.1.3-3

- Attempt to upload offline update file results in 504 Gateway Time-out.
    - Description: During the offline upgrade process, after the admin has downloaded an update file to their local environment when they try to upload this file, in rare circumstance, they may get a message stating “504 Gateway Time-out”. Despite this message, the file does get uploaded and the upgrade can proceed. The message is certainly annoying but the update process works correctly. The cause is mostly related to network traffic between admin’s local machine and their WebApp Secure machine. If this happens, just reload the update page and the correct status will be displayed.
- Backups feature requires that backups are always **one more day** than what is specified from UI/ configuration; so if administrator selects 1 day retention time, the backups will be retained for two days (default 24 hours, plus the 1 day designated in configuration).

Known Issues and Limitations with previous 5.1.x

- Cluster configuration upgrades in previous releases had two issues: a) regarding error messages during cluster upgrades and b) incorrect message on UI. Those issues are in the deployed code and we found them during our testing of upgrading from previous releases to 5.1.3, below is the workaround for the same when attempting cluster upgrades.
    - When updating clustered systems wherein each Traffic Processing node would log "An error occurred while attempting to obtain an error response from the factory: null" each time it tries to process the health check response. To resolve this problem, simply navigate to Configuration in the UI and 'Save' any configuration entry. This forces the configuration to be updated on each Traffic Processing Node, and the messages will cease.
    - When updating clustered systems wherein the update would randomly be marked as finished, even though all nodes haven't completed the update process. To fix this problem, re-initiate the update via the UI until it correctly displays the desired version (at the bottom of any the UI page).
    - We have fixed both the above issues in 5.1.3, so during the future upgrades of 5.1.3 to next release, above two issues will not occur.
- Due to an issue in internal services start/stop, sometimes during the upgrade from earlier 5.x.x releases to 5.1.3, one may notice messages such as the following messages. In such cases, the upgrade completes successfully and after a re-boot the system will function normally. These errors are in the past releases and will not impact functioning of 5.1.3.
    - “An error occurred while receiving a message in the consumer: alertcom.lambdaworks.redis.RedisException: Connection closed”
    - “[mws-config][ERROR] Error 111 connecting localhost:6767. Connection refused.”

Requesting Technical Support

To open a case or to obtain support information, please visit the Juniper Networks Support Site: http://www.juniper.net/support.