Release Date: 15ᵗʰ April, 2016

Release Notes

1. Two Factor Authentication introduced for GajShield Web UI login. New tab enabled for OTP configuration (Management → Administration → OTP Configuration).

   To configure two-factor authentication - [click here](#)

2. Network Zones introduced for firewall policy configuration (Configuration → Device → Zones).

3. Give priority of ISP globally and configure global failover under WAN Failover configuration (Configuration → WAN Failover → WAN Failover).

4. If DLP is configured then admin email ID will receive daily DLP upload summary report on email.

5. Option to configure Change Password link enable/disable option (when local database selected for userSense authentication), userSense page refresh time and redirect to specific URL after user is successfully logged in introduced. (Browsing → userSense → userSense Setup).

Bug fixes and Enhancements:

1. Firewall log under Diagnosis → Log Diagnosis → Firewall Logs will now show rule no., username, group name and device details.

2. Antispam mail logs in front-end will now show source ip address. (Reports → Mail Logs → Spam Detected and Reports → Mail Logs → Mail Archive).

3. No need to restart network for Static Routes add/edit/delete operations (Configuration → Static Routes & DNS → Routes).

4. Top Apps report will now show source-destination IP address. (Reports → Top Apps Report).

5. Option to reset Bandwidth quota for multiple users along with search option. (Browsing → Quota → Bandwidth Used).

6. 7z file upload block issue in DLP is now resolved.

7. Queue names restricted to alphanumeric and underscore (Definitions → QoS → Queues).

8. Cloud user logs issue (Gateway IP instead of client IP) is now resolved (Diagnosis → VPN Logs → Enterprise Cloud Logs).

9. No need to Restart Network for DNS server modifications Configuration → Static Routes & DNS → Nameservers).

10. DLP Alert email issue (username/group missing) for SMTP mails is now resolved.

11. Outlook and Yahoo Web-Mail block issue in DLP is now resolved.

12. SRC-DEST Port missing in Dos attack report for UDP traffic is now resolved. (Reports → Top DoS Attacks).

13. DHCP service will now be started only if configured.

14. Web Category for IP address can now be checked from GUI.

15. A confirmation (pop-up) will be asked for enabling GLOBAL Failover while adding/editing firewall rule with No Routing.

16. DLP template with single filter add issue is now resolved.

17. Source NAT is allowed if To Direction is ANY (Firewall → Policies → Rules).

18. Gateway IP will not be allowed to remove from interface if it's used in firewall rules/zones (Configuration → Device → Interfaces).

19. NTP configuration will now be enabled on all firewalls with default NTP server configured as pool.ntp.org (Management → NTP → NTP Servers).

20. Default Network Zone selected for LAN/WAN interface Configured from Quick Wizard.