Release Date: 27th June 2017

Release Notes

SECURE GUEST INTERNET MANAGEMENT SYSTEM

1. Guest User Network Management support:

   Overview

   Guest visitors to an enterprise, hotel, colleges or even public hotspots might need access to internet during their stay. The challenge faced by IT Managers is how to control and limit internet access of guest users without having to configure the guest's desktop and yet have a solution which is cost effective and easy to manage. IT Managers would need a solution which would provide a positive visitor experience without compromising the security of an enterprise.

   In providing internet access which could be for a day or even weeks during the stay of a guest, another challenge IT Managers face is creating temporary user IDs for guests. Maintaining such large changing list of users is tedious job for an admin. It is also difficult to apply access restrictions to these users, as user's database is frequently changing/getting updated.
   To know more click here

   Guest User Network Management configuration:
   (Browsing → Guest Users → Guest User Settings)
   (Browsing → Guest Users → Guest Users)

   SMS Gateway configuration integrated for guest users:
   (Management → Settings → SMS Gateway)

   Download of Guest User Registration logs available from Web-UI:
   (Management → Get Logs → Download Logs)

2. Option to change default time of GajShield's internal schedule activities like DLP upload summary report, Daily Internet activity report, Reset bandwidth quota, Reset time quota, Signature updates and Log cleanup. All these schedule activities perform in the night. Where office is complete shutdown with power off in the night. Because of this appliance is unable to perform all scheduled activities schedule in the night. To overcome this problem, now admin have rights to change the timing of schedule activities to their preferred timings. This can configure under:
   (Management → Settings → Schedule Activities)

3. MAC Filtering feature introduced with default whitelist/blacklist option. This feature is useful when admin wants MAC based control. With default whitelist MAC policy on LAN network, traffic from all MAC address in LAN network are allowed except blacklisted MAC address. Similarly using default blacklist MAC policy option, traffic from all MAC addresses on LAN network are blocked except whitelisted MAC addresses. This can configure under:
   (Firewall → Policies → MAC Filtering)

4. Configurable option is available to set email alert to administrator on Bandwidth Quota expiry.
   Using this option admin email will get alert if user's bandwidth quota is exceeded allocated quota limit.
   This configurable option is available under:
   (Browsing → Quota → Bandwidth Quota)

5. Option to configure L2TP over IPSec VPN on multiple ISP's. This option provides redundancy in terms of support of multiple ISP for L2TP configuration. Previously L2TP over IPSec tunnel can be configured on single ISP. Using this feature user can configure secondary ISP WAN IP in L2TP VPN configuration in case primary ISP is down. This can configure under:
   (VPN → L2TP → L2TP Options)

6. Download of ISP Failover (Up/Down status) logs available from Web-UI:
   (Management → Get Logs → Download Logs)

7. Option to download user-wise IM logs from Web-UI:
   (Reports → DLP Logs → IM Logs)

8. New Application/IPS signature update notification will come on Dashboard Alert Messages.

9. Option to change WAN Failover condition to TCP Port along with default PING option. This feature is useful when ISP is blocking PING request over the Internet and due to this admin is unable to use WAN Failover feature. To overcome this problem, this option is useful where GajShield will monitor ISP up/down status based on TCP port. If TCP (same as PING) mentioned port is not reachable then appliance will consider ISP link down and when TCP port is reachable then it will consider ISP link is UP on appliance. This can configure under:
   (Configuration → WAN Failover → WAN Failover)

Bug Fixes and Enhancements:

1. Improved option to view the usage status of Hosts/Host Ranges/FQDN Hosts/Networks/Network Groups defined with status like Active (if used in any policies) and Inactive (object is created but not used in any policies).

2. Added description field while adding DHCP static mapping entries:
   (Configuration → DHCP Server → Static Mapping)

3. Enhanced Cloud configuration to configure cloud server on NATed public IP where on GajShield WAN interface is configured with private IP:
   (Enterprise Cloud → Organization Information)

4. Option to view VPN tunnel host/network IP details in tooltip:
   (VPN → IPSec → Tunnels)

5. Option to enable/disable active directory user groups synchronization:
   (Configuration → User Management → Active Directory)

6. L2TP/PPTP VPN logs will show VPN user's source (public IP) details:
   (Diagnosis → VPN Logs → VPN Logs)

7. There was a problem in Bandwidth/Time quota when user belongs to multiple groups (in case of AD user group synchronization), this problem is now resolved.

8. New confirmation pop-up with Yes/No option for Global Failover while add/edit firewall rule.

9. Google Drive file upload block issue in DLP is now resolved.

10. DNS configuration issue from Quick Wizard is now resolved.

11. Improved email alert with clarification for Download limit exceeded.

12. Top Apps and Top App Users report under Top Reports will now show Source Port-Destination Port and Protocol details.

13. UserSense Bypass user's login/logout logs are coming frequently in current UserSense logs, ideally it should not come. This issue is now resolved.