Build v3.0 dc/nu series
Release date: 22 November 2017

RELEASE NOTES

Country/Country Group based policies

New country group specific policy template has been added in this new firmware version. You can now set firewall policies to block or allow rules for a particular country or for a country group in this new feature. Create a new country group template by going to
(Definitions -> Hosts -> Country Groups)
Using this feature, you can create firewall policies to block or allow a particular country or group of countries based on source and destination. You can do this by going to
(Firewall -> Policies -> Rules)

New tab Port Forwarding

Port forwarding allows remote computers (for example, computers on the Internet) to connect to a specific computer or service within a private local-area network (LAN).
New tab has been added in this firmware version for port forwarding which makes it easier to configure and specify details like internal IPs, external IPs, services to configure port forwarding firewall rules easily. You can now use the improved and easier port forwarding option by going to
(Firewall -> Policies- > Port forwarding)

Option to enable console access for admin users

Earlier only the super user was authorized to access console. We have now added an option for super user, when they create sub-admin users, they can have the option to grant console access for sub-admin users. You can configure this access by going to
(Management -> Administration -> Manage Admins)

Option to block password protected files in DLP (zip, pdf)

You can now block password protected files in DLP by selecting Generic service and specifying “Attachment” option and selecting the appropriate file extension (zip or pdf). This option has now been added which will help you block even password protected files with the extensions .zip, .pdf. Access option to block password protected files in DLP by going to
(DLP -> DLP policies -> DLP Template)

Admin IP's can now be configured for individual admin

Super user has the access to bind sub admin users to single or multiple IP addresses to be given access to GajShield WebUI. Admin will get access to GajShield WebUI only from the added IP addresses. Admins or the super user won’t be able to access the GajShield WebUI if not accessed via one of those specified IP Addresses. Super user can bind IP addresses by going to
(Management -> Administration -> Admin IPs)

Change Password Link provided in dashboard Alert Console for Default Password

In case your firewall is still been authenticated using the default password, we have now added a link in dashboard to change the default password in the new firmware version. To change the password go to
(Dashboard -> Alert messages and click on “Click here to change” link)

L2TP users can now be authenticated through AD, and LDAP

L2TP over IPsec VPN users can now be authenticated through third party authentication servers such as AD and LDAP, configure it by going to
(Configuration -> User Management.)
After configuring the third party authentication server, In order to integrate AD or LDAP for L2TP server, configure it by going to
(VPN -> L2TP -> L2TP Options)

SMTP Mails blocked through DLP can now be released from Antispam Mail Archive Logs

Earlier, once a mail was blocked through DLP Engine, it wasn't available for viewing. In this new firmware version, you can now view the mails that have been blocked using DLP Engine under the Antispam mail archive logs. In order to view or release the mails that have been blocked using the DLP Engine, go to
(Reports -> Mail Logs -> Mail Archive)

Multi-select option enabled to delete Daily PDF Reports

Using the multi select option, you can now delete daily PDF reports with ease.
To delete multiple daily PDF reports, go to
(Reports - > Browsing -> Daily PDF Reports)

Added VPN Logs in Misc Options

To preserve the VPN logs for specified days, we have now added a new field called "Days to Preserve VPN Logs"under misc option. In order to set the new field, go to
(Management -> Settings -> Misc Options)

Bug Fixes and Enhancements:

Proxy mode browsing issue with Chrome-61 browser is now resolved

SSL Certificate error for the specific https URL accessed using proxy mode in the new Chrome 61 browser has been resolved.

URL QoS failover issue is now resolved

Enhancements in URL QoS failover feature.

Zip file block issue in DLP is now resolved

Earlier, there was a problem to block zip files in SMTP mail using DLP engine. We have now resolved this issue and zip files can now be successfully blocked.
(DLP -> DLP Policies -> DLP Template)

Static Routes replication issue in HA is now resolved

There was a problem with respect to adding routes in the HA. When we added routes in master firewall, they got synchronized in backup firewall but in actual the routes weren't added in the backup firewall. This problem has now been solved.
(Configuration ->Static Routes and DNS -> Routes)

DHCP service issue with large subnet is now resolved

Earlier, there was an issue with configuring large subnet in DHCP Configuration which has now been solved.
(Configuration -> DHCP Server -> DHCP Server Config)

IPsec VPN tunnel clone issue is now resolved

There was a problem with respect to cloning of VPN Tunnel where IKE version was not reflecting while cloning VPN tunnel. This issue has not been resolved. Access it by going to
(VPN -> IPsec -> Tunnels)

DHCP IPv6 Static Mapping add issue is now resolved

Earlier there was a problem while adding IPv6 Static mapping in DHCP. We have now resolved that. Access it by going to
(Configuration -> DHCP Server -> Static Mapping)

WAN Failover issue with TCP settings is now resolved

Earlier there were problems with respect to WAN failover issues in TCP settings which have now been resolved. You can view the improved settings by going to
(Configuration -> WAN Failover -> WAN Failover)

Loop-back NAT rule issue with special services is now resolved

While creating Loop-back firewall rules with special services, previously, the rules wouldn’t work. These problems have now been resolved.
(Firewalls -> Policies -> Rules)

DLP upload logs issue in DLP is now resolved

In DLP reports when a mail was sent using yahoo webmail with an attachment, then in DLP webmail reports earlier, the attachments weren’t been shown and attachments were coming separately in DLP upload logs. This problem has now been resolved. Additionally, now attachments and mail are shown together.
(Reports -> DLP Logs -> DLP Mail Logs)

Read-only admin with Reports (exception) doesn't work issue is now resolved

When admin user was been created with report options, certain report accesses weren’t visible properly.
This problem has now been resolved.

Gmail sender-id missing in Web-Mail logs issue is now resolved

When email was sent using gmail through web, then in DLP Web Mail reports, the sender id wasn’t visible. This issue has been resolved now.
(Reports -> DLP Logs -> DLP Mail Logs)

OneDrive file upload block issue is now resolved

The file upload block issue with respect to OneDrive has now been solved in DLP.