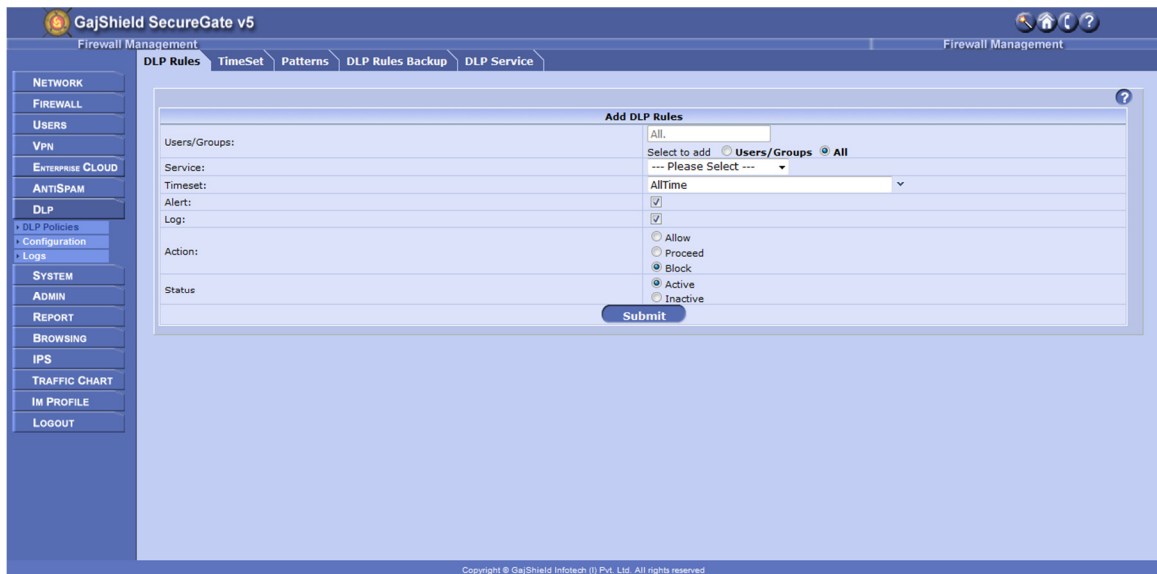




# How to create DLP Policy on firewall

**Note:** Before creating DLP policies on GajShield, make sure you have DLP license. Create SSL certificate & firewall policies with http & https transparent proxy.

1. Go to DLP Rules & click on  to add a new policy, as seen below.



- **Users/Group:** Select **Users/Group** radio button, to add users or group for DLP scanning or Select **ALL** radio button, to enable DLP scanning for the entire network.
- **Services:** Select the service from the drop down list to enable DLP, also Set Filters to drill down to the exact matching data, by clicking on  to remove Filters click on . If there are no filters set in DLP rule, it will capture complete data for the DLP rule configured.
  - Generic: All http & https traffic going through the firewall are monitored.
    - Http: Captures http header level data.
    - SMTP: Smtip header level data is captured.
    - File Upload: All uploads from http & https are scrutinized by the firewall.
  - Web Mails: View or Block access to Personal emails. Mails of the below mentioned web clients can be seen word by word with attachments.
    - Gmail
    - Yahoo
    - Rediff

- MSN Live
  - Sify Mail
- Orkut: Log data going through Social Networking Sites, with all the below options covered.
  - Orkut Scrap
  - Orkut Message
  - Orkut Forum Post
  - Orkut Forum Event
- Facebook: Popular used Social Networking site for business, now keep track of data going out of Facebook, with all the mentioned optioned covered.
  - Facebook Wall
  - Facebook Message
  - Facebook Forum Post
  - Facebook Comment
  - Facebook Note
  - Facebook Event
- IM Chat: Chats & file upload happening through below mentioned IM clients can be recorded on the firewall.
  - Yahoo Chat
  - Jabber Chat
  - MSN Chat
  - Gadu Chat
- Web Chat: Web chats are handy tools, used on Web 2.0. Transcription also possible of the below mentioned Web chats clients.
  - Yahoo Web Chat
  - Gmail Web Chat
  - Orkut Web Chat
  - Facebook Web Chat
- SMTP Mails: Log the entire mail with attachment, to analyze Data leak. Works on port 25.
  - SMTP Mails
- **Timeset**: Set timeline for DLP rules to monitor data (default timeline is 24 hours monitoring enabled. Recommended) or set new time line according to your requirements.
- **Alert**: Set email alerts for DLP communications. Example alerts on file upload, email sent from personal web mail, etc.
- **Log**: Enable check box to capture & view outbound DLP data.

- **Action:** Action to be assigned to a DPL Policy.
  - Allow: Allow access if criteria matches to DLP policy.
  - Proceed: Scans DLP policy & push down for further more scanning through other DLP policies.
  - Block: Will deny access to the said policy & will log the same.
- **Status:** Decide whether the rule should be active or inactive.
  - Active: DLP engine passes data through active DLP policies.
  - Inactive: Inactive DLP policies are bypassed by DLP engine.

**Note:** After making changes in DLP Policies, restart DLP services for the changes to take effect.

2. To monitor chats & uploads through IM messengers, need to configure IM settings.



- **Port For Redirected Connections (default 16667):** IM clients communication ports are intercepted to port 16667 for DLP engine to scrutinize data.
- **Badwords Replace Character:** Bad words will be replaced with the character, inserted in the text box. Default is an asterisk.
- **Badwords Block Count:** If a message contains more than this many bad words then the message will be completely blocked & not just replaced.
- **File Transfer (Only for Jabber / Gtalk, yahoo, msn):** Control on File Transfer through IM, above mentioned IM clients supported.
- **Webcams (Only for yahoo):** Block Video chats through GajShield DLP.
- **SSL support (Only for Jabber / Gtalk):** Record chat on encrypted protocol.

- **Protocol Settings:** Mentioned IM protocols are scanned by GajShield DLP engine.
  - Jabber / XMPP / Gtalk
  - Yahoo
  - MSN
  - Gadu-Gadu
  - ICQ / AIM
  - IRC
- **Bad Word Filtering:** There are bad word database by default on GajShield firewall, bad words can be manually entered in the firewall, by clicking on [\(Add new\)](#) next to **Available bad words** & after adding the bad word move it to **Selected bad words** column.

**Note:** After making changes in IM Configuration, restart IM services for the changes to take effect.

For further assistance please Contact GajShield Support on +91 22 66607450 / 51/ 52/ 53

Email: [support@gajshield.com](mailto:support@gajshield.com)