How to Configure Mail Gateway Service Limits

For the Mail Gateway service, you can set limits for mail that is received and delivered. To help prevent against Denial of Service (DoS), you can also set limits on the number of inbound and outbound connections.

Configure Mail Gateway Service Limits

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Mail-Gateway > Mail Gateway Settings**.
2. In the left menu, select **Limits**.
3. Click **Lock**.

4. In the **Mail Gateway Limits** section, set limits for mail that is received and forwarded. You can configure the following settings in this section:

Setting	Description
Limit Mail Data Size	To limit the size of mail data (attachments), select **yes**. In the **Mail Data Size (MB)** field, enter the maximum size for mail data.
Mail Data Size (MB)	The maximum size of mail data in MB (default: 20). If the mail size exceeds this limit, the mail gateway refuses delivery and sends an error message to the sender. This setting reflects the actual mail body size because SMTP applies transfer encoding. The actual mail size may be greater than the physical size of the attachment. For example, if you add an attachment that is about 5 MB, the total mail size can be up to about 6.5 MB.
DSN for Max Data Size Excess	If you want the mail gateway to create an extended Delivery Status Notification (DSN) message when an email has exceeded the maximum allowed size that is specified by the **Mail Data Size (MB)** setting, select *yes*.
Maximum Number of Recipients	The maximum number of recipients of mail. Because RFC2821 requires at least 100 possible recipients of mail, you cannot enter a limit that is lower than 100 (default: 200).
DSN for Max Recipients Excess	If you want the mail gateway to create an extended DSN when an email has been forwarded to more recipients than the limit specified by the **Maximum Number of Recipients** setting, select **yes**.
Refuse Empty Mail from	By default, the SMTP server accepts all incoming emails. To reject emails with empty sender information, select **yes**.
Accept Loose Domain Name	Domain names may only contain the following characters: [-.0-9A-Za-z]. From the **Accept Loose Domain Name** list, select one of the following options to specify if domain names are checked for incorrect syntax. ◦ **no –** Domain names are checked. Emails are rejected if their domain names use incorrect syntax. ◦ **yes –** Domain names are not checked. Emails with domain names that use incorrect syntax are delivered.
Max. Attachments	The maximum number of to-be-scanned attachments per MIME email.
Drop Mails over Attachment Limit	To drop emails that contain more attachments that the limit specified by the **Max. Attachments** setting, select **yes**.
Drop Fragmented Mails	To reject malformed and damaged emails, select **yes**.
Max Age of crashed Mails (d)	The maximum number of days that emails can stay in the 'crashed' directory.

Max. SMTP Line Length	The maximum number of characters per line. Barracuda Networks recommends that you use the RFC maximum limit of 1000 characters.
Max. Received From Lines	The maximum number of *From:* headers. Default: 20. Emails that are sent over more hops than this limit are are discarded and logged: `Warning LOOPDROP from <some@email.com> id 20160101-020242-18795-00`
Max. Header Lines	The maximum number of header lines. Default: 100. Emails that have more then the max header lines in its header are discarded and logged: `Warning LOOPDROP from <some@email.com> id 20160101-020242-18795-00`

5. In the **DoS Protection** section, set limits on the number of parallel inbound and outbound connections. You can configure the following settings in this section:

Settings	Description
Parallel Inbound Connections | Parallel Outbound Connections	The maximum number of parallel inbound or outbound connections for receiving mail (default: 5). If your mail gateway handles a lot of mail traffic, you may need to increase this value. (These values must not be 0.)
Parallel Outbound Connections | Parallel Outbound Conn. per Peer	The maximum number of parallel TCP connections from a single inbound or outbound source IP address (default: 25). This provides effective protection against DoS attacks. ◦ These values must not be **0**. ◦ The number of maximum parallel connections per peer may not be greater than the maximum number of parallel connections. ◦ To generate the `Resource Limit Exceeded: Max connections (per Peer) [136]` event when the limit values are exceeded, select *yes* from the **Parallel Connection Limit** list in the mail gateway reporting settings. For more information, see How to Configure Mail Gateway Reporting.

6. Click **Send Changes** and **Activate**.

Continue with How to Configure Mail Gateway Reporting.