How to Use the Mail Gateway Interface

https://campus.barracuda.com/doc/53248814/

The following article explains the functional parameters accessible via the Barracuda NextGen Firewall F-Series Mail Gateway interface. For each tab there is a context menu accessible that allows specifying the settings according to your needs.

To access and administer operative processes on the Barracuda NextGen Firewall F-Series mail gateway, click **MailGW** in the box menu. The user interface is characterized by the following tabs:

Mail Queue Tab

This register displays pending mail jobs. In section view mails jobs are arranged according to their spam classification state. They are classified into the following categories:

- **Spam State Unknown**
- **Spam**
- **No Spam**

> If no SPAM Filter has been configured, all emails are categorized as *Spam State Unknown*, regardless of their content.

Information on currently queued jobs covers the following:

Parameter Overview

Column	Description
Spam	Emails are flagged with an icon according to their spam classification: • **Yellow** – Spam State Unknown • **Red** – Spam • **Green** – No Spam
From	Shows the sender address.
To	Shows the recipient(s) address(es).
Subject	Shows the mail object's subject.

State	Shows an icon displaying the current spool activity and a corresponding state description: • **Green Arrow** – Active pending, ready for delivery and pending until MTA is ready. • **Yellow Arrow** – Active, delivery is performed right now. • **Exclamation Mark** – Give up, email could not be delivered due to problems on the recipient's side and no further delivery attempts will be undertaken. • **Yellow bug** – Crash, email could not be delivered due to misconfiguration (for example missing MX record, unknown recipient domain) • **Grey data icon** – Pause, delivery has been paused due to execution of the admin command Pause Delivery (see **Context Menu Entries**)
Prio	Shows the priority of the mail object: • **Green** – Low • **Orange** – Normal (default) • **Red** – High • **Clock** – Urgent
APrio	Shows the actual priority of the mail object. Due to high traffic a mail object can be ready for delivery but cannot be delivered yet. The object's priority continuously rises, until it can finally be sent. Effective priorities in the APrio column are the same as in the Prio column, except for priority urgent.
Size	Shows the size of the mail object.
NumTo	Shows the number of recipients for the mail object.
Tries	Shows the tries carried out for delivering the mail object.
Last Status	Shows the last try's status.
Next Try column	Shows waiting period until next delivery try (hh:mm:ss).
Last Try	Shows time passed since last delivery try.
Receive Time	Shows receiving time of the mail object.
Scan State	Shows an icon displaying the email objects scan state. The following icons are in use. • **Green shield** – Email scan has been completed successfully. • **Red cross shield** – Email scan could not be executed completely and has been aborted.
Spool ID	Shows the ID of the mail object.

Context Menu Entries

Right-clicking a data set opens a context menu with commands assisting in figuring out why a mail could not be delivered and allowing influence on execution of pending mail jobs.

> Execution of the commands made available through the context menu requires adequate permissions.

The following options are available:

Parameter Overview

Parameter	Description
Show Envelope	This command opens a window showing the mail envelope. The mail envelope contains information on the selected mail job, such as sender / recipient address, helo / ehlo name, mail size, scheduling priority
Show Log File	This command opens a window showing the mail job's log file. The log file contains information on MTA operation.
Schedule Now	If an email cannot be delivered at once, the mail gateway retries delivery according to the MTA Retry Sequence. To skip the MTA Retry Sequence select this option to start a new delivery attempt.
Change Priority	With this option you can change scheduling priority of the selected mail job. Default scheduling priority is normal. Jobs with high priority will be scheduled first; jobs with lower priorities will be scheduled thereafter. The following scheduling priorities exist: • **Low** • **Normal (default)** • **High** • **Urgent**
Change Priority and Schedule	This option combines the two scheduling options: • **Change Priority** • **Schedule Now**
Pause/Resume Delivery	Select **Pause Delivery** to halt delivery of a mail job.
	Select **Resume Delivery** to resume it.
Discard Mail	Select this option to discard a mail job and to remove the mail object from the mail queue. Mails in active state cannot be discarded.

Access Tab

This register shows the access cache of the mail gateway service. The access cache contains completed mail jobs, which have been moved to it from the mail queue. The access cache thus represents a history of the mail gateway. The maximum number of entries the access cache may contain is specified through parameter sets MailGW Settings - Limits – see: How to Configure Mail Gateway Service Limits. Again, in section view, emails are arranged in groups disclosing their spam classification state. Mails are classified into the following categories:

- **Spam State Unknown**
- **Spam**
- **No Spam**

All columns, except the **State** column, can be interpreted in the same way as described in the section **Mail Queue Tab**. As the **Access** tab represents a history, the state column only knows the following three states:

- **deliver** – mail has been delivered successfully
- **giveup** – mail could not be delivered / mail has been discarded by admin command
- **crash** – an error has occurred during delivery or internal operation

Furthermore, the following column pays regard to handling of suspicious and malicious attachments:

- **Stripped column** – A mail object is tagged with a pair of scissors, if a spam suspicious or malicious virus attachment has been removed from it.
  All attachments will be cut out from an email containing multiple attachments, if only one of them is classified as suspicious file because it cannot be scanned. The virus scanner does not generate information, which of the files is the suspicious one. If of interest, a manual scan is necessary, after all attachments have been downloaded. For a definition of suspicious files, please see section: **Delete All Suspicious Attachments**.

Context Menu Entries

Execution of the commands made available through the context menu requires adequate permissions.

Right-clicking a group title makes the following context menu entries available:

- **Delete Items in Category** – Deletes all access entries from the selected category Spam State Unknown, Spam or No Spam.
  This action does not automatically delete possibly cut attachments from the **Attachments** tab. Right-clicking any data set makes the following context menu entries available:
- **Show Logfile / Show Envelope** – See above section, **Context Menu Entries.**
- **Remove Entry** – Removes the selected data set (or multiple data sets if selected).
- **Clear All** – Deletes all objects from the **Access** tab.

Right-clicking a data set flagged with in the **Attachment Stripped** column makes the following additional option available:

- **Show Stripped Attachments** – Clicking this item redirects the administrator to the attachment(s) cut from the mail object, now located for analysis in the **Attachments** tab (see below section, **Attachments** Tab).

Spam Tab

This tab combines Mail Queue and Access tab and only displays spam tagged emails. As this tab serves informational purpose only, the context menu has no tools for modification/deletion of entries. The only available actions from the context menu are:

- **Show Envelope** – Opens a view containing basic information concerning the select mail (for example mail size, peer IP address, sender,).
- **Show Log File** – Opens a view containing all log files that were created by the selected mail.

The columns building the spam list/spam tab can be interpreted in the same way like the ones used in the **Mail Queue Tab** and **Access Tab** (see above section, **Access Tab**).

Processes Tab

The **Processes** register shows the active mail gateway processes. When a multitude of processes is running, use the filter options **Delivery**, **Receiving**, and Internal in the filter section area, to limit the amount of processes shown.

Internal processes are not shown by default. Adapt the filter setting for Internal to display them.

Information on currently active processes covers the following:

Parameter Overview

Parameter	Description
PID column	Shows the Process Identifier. (Proc ID)
State column	Processes can have the following states: • **pause** (only available with type mgw_main) • **active**

Type column	The following process types exist: • **mgw_main** – This is the parent process of the Barracuda NextGen Firewall F-Series mail gateway service. It provides the SMTP listening sockets and handles the mail receiving processes (SMTP worker processes). • **qspool_main** – This process listens for incoming connections from a remote host running the Barracuda NextGen Firewall F-Series administration GUI Barracuda NextGen Admin. • **qspool worker** – This process is responsible for transferring the visualization data (Mail Queue, Access Cache, Processes, Logs, Stats) to the remote host running the Barracuda NextGen Firewall F-Series administration GUI Barracuda NextGen Admin. • **SMTP worker** – This temporary process is activated when a client opens a SMTP connection to the mail gateway. The SMTP worker process is responsible for receiving mail data from the client. It terminates when mail data transfer has ended. • **spooler** – The spooler process is responsible for scheduling mail jobs. When the worker process receives a mail job, its state temporarily changes to spool. While it is in this state, the mail job is visualized in the **Mail Queue** tab. The mail queue becomes larger with every mail job getting spooled. The sequence, by which the spooled items are worked off, is handled by the **Spooling Priority**. • **mta (Mail Transfer Agent)** – This process is responsible for mail delivery. When the MTA process receives a mail job from the spooler, it establishes a connection to a foreign target mail server (the mail job's recipient mail server) and delivers the email. After successful delivery, the mail job moves from the mail queue to the access cache. • **ha (High Availability)** – This process is needed for synchronizing mail traffic between HA partners.
Peer column	Shows peer IP and port handled by a SMTP or qspool worker.
Spool ID column	Shows the spool ID of the mail being processed by a **M**ail **T**ransfer **A**gent (MTA).

Context Menu Entries

Execution of the commands made available through the context menu requires adequate permissions.

Right-clicking a data set makes the following context menu entries available:

- **Kill Process** – With administrative permissions single worker processes can be killed. MTA processes are automatically created on demand until the configured maximum number of MTAs has been reached (see: How to Configure Advanced Mail Gateway Settings, section **Mail Transfer Agents (MTAs)**).

  Killing a worker process triggers the event *Subprocess Kill Requested: Kill PROC_SMTP Worker [2054]* when eventing is activated through parameter **Kill Worker Process** (default: **no**).
- **Allow Mail Reception** – Used to resume mail operation after blocking mail reception.

- **Block Mail Reception** – Used to block the mail gateway process.

Attachments Tab

The Attachments tab assembles cut email attachments. Its listing arranges mail objects sorted ascending by their Spool ID. Cut attachments are directly assigned to the object they have been cut from. Use this operative area to decide individually how to proceed with suspicious or malicious files.

File types meant to be cut from emails and not forwarded to their recipients are on the one hand defined through the virus scanner (see: Virus Scanner) and on the other hand specifically appointed through the mail gateway settings (see: How to Configure Content Stripping, Grey Listing, and Blacklists section **Attachment Stripping**).

Available information is arranged in the following columns:

- **Spool** – This column shows the email's spool ID and behind it in brackets the number of attachments which has been cut from it. Click on the + symbol to display detail information regarding the attachments.
- **From** – Shows the sender address.
- **To** – Shows the recipient(s) address(es).
- **Subject** – Shows the mail object's subject.
- **Receive Time** – Shows the time the message has been arrived at the mail gateway.
- **Filename** – Shows the name of the file, which has been cut.
- **Reason** – Displays the reason why the file has been cut.

Context Menu Entries

Right clicking any data set makes the following context menu entries available:

Parameter Overview

Parameter	Description
Delete All Attachments	Deletes all attachments from all mail objects currently assembled in the listing regardless of the reason why they have been cut.
Delete All Normal Attachments	If the mail gateway has been configured to cut all file attachments regardless of their type (see: How to Configure Content Adaptions, section **Attachment Stripping**), they will be contained in this tab. This action deletes all mail attachments, which have been stripped off according to mail gateway settings.

Delete All Suspicious Attachments	Deletes all file attachments, which have been classified as suspicious by the virus scanner. Files are classified as suspicious when the virus scanner for any reason is not able to handle them properly. Amongst others, the following can be causes for this: • The file attachment is larger than 1 MB and thus cannot be scanned completely. • The file attachment is encrypted. • The file attachment is an archive file exceeding the maximum allowed archive size.
Delete All Virus Attachments	Deletes all malicious file attachments like viruses.
Right-clicking a **Spool ID** header makes the following action available:	• **Delete Attachments From This Mail** – Deletes all attachments from the selected mail object.
Right-clicking a selected file object makes the following actions available:	• **Get Attachment** – Makes the cut attachment available for download. It is up to the respective administrator to download the file to his/her own harddisk, scan the file manually and thereafter possibly forward it to the original recipient. • **Delete Attachment** – Deletes the selected file attachment.

Continue with: How to Use the Grey Listing Tab.