MAILGW Tab

https://campus.barracuda.com/doc/51184507/

The Barracuda NextGen Admin **MAILGW** tab allows you to view and administer operative processes on the Barracuda NextGen Firewall F-Series mail gateway. The **MAILGW** tab is only accessible when the Mail Gateway service is introduced and configured on the F-Series Firewall. For more information, see Mail Gateway. To navigate through the sections on the **MAILGW** page, click the tabs. For each tab there is a context menu accessible that allows specifying the settings according to your needs. Execution of the commands made available through the context menu requires adequate permissions.

Mail Queue tab

This tab displays pending mail jobs, arranged according to their spam classification state:

- **Spam State Unknown** – (Yellow) Unknown state. If no SPAM Filter has been configured, all emails are categorized as *Spam State Unknown*, regardless of their content.
- **Spam** – (Red) Classified as SPAM.
- **No Spam** – (Green) Classified as not SPAM.

Information on currently queued jobs covers the following:

- **Spam** – Emails are flagged with a colored icon according to their spam classification.
- **From / To** – Shows the sender / recipient(s) address.
- **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 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** – The number of recipients for the mail object.
- **Tries** – The number of tries carried out for delivering the mail object.
- **Last Status** – Shows the status of the last try.
- **Next Try** – Shows the waiting period until the next delivery try (hh:mm:ss).
- **Last Try** – The time passed since the last delivery try.
- **Receive Time** – The receiving time of the mail object.
- **Scan State** – Shows an icon displaying the email object's 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** – The ID of the mail object.

Context menu entries

Right-clicking a data set opens a context menu with commands that help to find out why a mail could not be delivered and that influence execution of pending mail jobs:

- **Show Envelope** – 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, and scheduling priority.
- **Show Log File** – 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 the scheduling priority of the selected mail job. Default scheduling priority is **Normal**.
- **Change Priority and Schedule** – This option combines the two scheduling options **Change Priority** and **Schedule Now**.
- **Pause/Resume Delivery** – Select **Pause Delivery** to halt delivery of a mail job; select **Resume Delivery** to resume it.
- **Discard Mail** – Discards the mail job and removes the mail object from the mail queue. Mails in active state cannot be discarded.

Access tab

This tab shows the access cache of the Mail Gateway service. The access cache contains completed mail jobs that have been moved to it from the mail queue. The maximum number of entries the access cache may contain is specified in **MailGW Settings > Limits**. For more information, see: How to Configure Mail Gateway Service Limits. Emails are arranged in groups disclosing their spam

classification state. Since 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

The **Stripped** column regards the handling of suspicious and malicious attachments. A mail object is tagged with a pair of scissors if spam or a suspicious or malicious virus attachment has been removed from it.

All attachments will be cut out from an email containing multiple attachments, even if only one of them is classified as suspicious file because it cannot be scanned. The virus scanner does not generate information regarding which of the files is the suspicious one. If a file is suspicious, a manual scan will be necessary after all attachments have been downloaded. For a definition of suspicious files, see **Attachments tab**, setting: **Delete All Suspicious Attachments**.

Context menu entries

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.
  - **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 within the **Attachment Stripped** column makes the following additional option available:

- **Show Stripped Attachments** – Redirects the administrator to the attachment(s) cut from the mail object, now located for analysis in the **Attachments** tab.

Spam tab

This tab combines **Mail Queue** and **Access** tab and only displays spam tagged emails. Since this tab serves informational purposes 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 selected 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.

Processes tab

The **Processes** tab shows the active mail gateway processes. Internal processes are not shown by default. Use the filter options **Delivery**, **Receiving**, and **Internal** in the filter section area to customize the view.

Information on currently active processes is covered in the following columns:

- **PID** – Shows the Process Identifier. (Proc ID)
- **State** – Shows the process state. State **pause** is only available with type mgw_main.
- **Type** – The following process types exist:
  - **mgw_main** – This is the parent process of the 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 firewall 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 Barracuda NextGen Admin.
  - **SMTP worker** – This temporary process is activated when a client opens an 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** – This process is responsible for scheduling mail jobs. When the worker process receives a mail job, its state temporarily changes to spool. While in this state, the mail job is visualized in the **Mail Queue** tab. The mail queue becomes larger with every mail job 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 -mail. 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** – Shows peer IP address and port handled by an SMTP or qspool worker.
- **Spool ID** – Shows the spool ID of the mail being processed by a **M**ail **T**ransfer **A**gent (MTA).

Context menu entries

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. For more information, see How to Configure Advanced Mail Gateway Settings. 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. Mail objects are sorted in ascending order 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 defined through the virus scanner and specifically appointed through the **Content Adaption > Attachment Stripping** settings in the mail gateway configuration.

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 that 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 arrived at the mail gateway.
- **Filename** – Shows the name of the file that 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:

- **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** – Deletes all mail attachments that have been stripped off according to the **Content Adaption > Attachment Stripping** settings.
- **Delete All Suspicious Attachments** – Deletes all file attachments that have been classified as suspicious by the virus scanner. Files are classified as suspicious when the virus scanner is not able to handle them.
  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, afterwards, possibly forward it to the original recipient.
- **Delete Attachment** – Deletes the selected file attachment.

Continue with: How to Use the Grey Listing Tab.