Content Analysis - Outbound Mail

https://campus.barracuda.com/doc/3211296/

See Regular Expressions for advanced filtering text patterns. HTML comments and tags in message HTML source are filtered out so that content filtering applies to the actual words as they appear when viewed in a web browser.

See Outbound Quarantine for more information on messages can then be viewed, delivered, rejected, deleted, or exported from the **Overview > Outbound Quarantine** page.

If you make setting changes, allow a few minutes for the changes to take effect.

Attachment Filters

All outbound messages, including those from exempt senders, go through attachment filtering. On the **Outbound Settings > Content Policies** page, you can select to filter text matching the entered pattern based on **File Name** or **MIME** type, and select whether to **Block**, **Ignore**, or **Quarantine** outbound messages. Additionally, you can select to **Block**, **Ignore**, or **Quarantine** attached archive files that require a password to unpack.

Password Protected Archive Filtering

For outbound mail, you can select to block, quarantine, or ignore messages containing archive file attachments. Selecting **Ignore** means that the service does not look for, or act on, emails with attachments that require a password to unpack.

Password Protected Microsoft Documents

For outbound mail, you can select to block, quarantine, or ignore messages containing password protected Microsoft documents. Selecting **Ignore** means that the service does not look for, or act on, emails that contain password protected Microsoft documents.

Password Protected PDF Documents

For outbound mail, you can select to block, quarantine, or ignore messages containing password protected PDF documents. Selecting **Ignore** means that the service does not look for, or act on, emails that contain password protected PDF documents.

Message Content Filters

Customize content filtering based on any combination of subject, headers, body, attachments, sender, or recipient, and apply to outbound mail. See the **Outbound Settings > Content Policies** page for settings. Filter actions for outbound mail include **Block**, **Allow**, **Quarantine**, **Encrypt**, and **Do not encrypt**.

Messages that meet the **Quarantine** criteria are sent to the Outbound Quarantine for the administrator to evaluate. Messages can then be viewed, delivered, rejected, deleted, or exported from the **Overview > Outbound Quarantine** page.

Enter filter patterns and select to **Block**, **Allow**, **Quarantine**, **Encrypt**, or **Do not encrypt** for **Subject**, **Headers**, **Body**, **Attachments**, **Sender**, or **Recipient**. Note that Header filters are applied to both the header name and content of any header, while the Subject filters only scan the contents of the Subject header. Use regular expressions as well as the following special characters:

. [ ] \ * ? $ ( ) | ^ @

When using the above special characters, you must escape each character with a backslash ("\").

Attachment Content Filtering is limited to text type files such as most MS Office files, html, pdf files, and other document files.

Predefined Filters

Select a predefined data leakage patterns (specific to the United States) for **Subject**, **Headers**, **Body**, or **Attachments**. Select whether to **Block**, **Quarantine**, or **Encrypt** outbound messages based on the filter.

Order of Precedence for Attachment Filters, Message Content Filters, and Predefined Filters

The Attachment Filters, Message Content Filters, and Predefined Filters support the following actions, in the following order of precedence:

Order	Filter	Action

1	Message Content Filter	Allow
2	Message Content Filter	Block
3	Predefined Filter	Block
4	Attachment Filter	Block
5	Attachment Filter	Quarantine
6	Message Content Filter	Quarantine
7	Predefined Filter	Quarantine
8	Message Content Filter	Do not encrypt
9	Message Content Filter	Encrypt
10	Predefined Filter	Encrypt

Note that when you select **Do not encrypt** on a **Message Content Filter** and **Encrypt** on a **Predefined Filter**, the Message Content Filter exemption takes precedence over the Predefined Filter and the message will not be encrypted.

Predefined Filter Exceptions

Add exemptions to predefined HIPAA or Privacy content filters to prevent outbound emails that include phone number or street address items from being blocked, quarantined, or encrypted.

Image Analysis

Image analysis techniques protect against new image variants. Image analysis is automatically configured in the Barracuda Email Security Service.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.