Content Analysis - Inbound Mail

https://campus.barracuda.com/doc/96023007/

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

Email Gateway Defense enables administrators to set custom content filters for inbound messages based on message content and attachment file name or MIME type, and specify whether to block, quarantine, or ignore password protected archive files and messages containing password protected Microsoft attachments. See the **Inbound Settings > Content Policies** page for settings.

Attachment Filters

For inbound mail, you can filter attachments based on **File Name** or **MIME Type**.

Password Protected Archive Filtering

For inbound 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 inbound 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 inbound 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

Base message content filtering on any combination of subject, headers, body, attachments, sender or recipient filters, and you can specify actions to take with messages based on pre-made patterns (regular expressions) in the subject line, headers, message body, sender or recipient lines. See Regular Expressions for text patterns you can use for advanced filtering.

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

Note that HTML comments and tags embedded between characters in the HTML source of a message are filtered out so that content filtering applies to the actual words as they appear when viewed in a web browser.

For information about content filtering for outbound messages, see Content Analysis - Outbound Mail.