Content Analysis Outbound

https://campus.barracuda.com/doc/3866721/

Custom Content Filters

Custom content filtering based on the subject line, message headers, message body and attachment file type can be applied to outbound mail just as it can be to inbound mail. See the filtering pages on the **BLOCK/ACCEPT** tab for details on settings. Note that, in addition to *block* and *quarantine*, filter actions for outbound mail include *encrypt* and *redirect*.

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

Attachment Content Filtering

All outbound messages, including those from whitelisted senders, go through attachment filtering. You can block, quarantine, encrypt or redirect outbound messages that contain attachments which include text matching the patterns you enter here. Attachment Content Filtering is limited to text type files such as MS Office files, html, pdf files and other document files. A notification will be sent to the sender when an outbound message is blocked due to attachment content filtering.

Blocking attachments with macros

For MS Office documents, you can set **Block Macros (MS Office Attachments)** to **Yes** if you want to block all attachments that include macros. This feature applies to both inbound and outbound mail.

DLP and HIPAA Compliance

You can also take actions with outbound messages that contain matches to pre-made patterns in the subject line, message body or attachment. With information types such as:

- Credit card patterns,
- Social security numbers (USA only),
- Combinations of privacy information such as birthday and driver’s license, and
- Diagnosis/prognosis as defined under HIPAA

...the Barracuda Email Security Gateway can filter attachment content and encrypt, block, quarantine, allow or redirect messages as configured on the **BLOCK/ACCEPT > Content Filters** page. Note that the format of this data varies depending on the country, and these filters are more commonly used in the U.S.; they do not apply to other locales.

Fingerprint Analysis

Outbound messages can undergo Fingerprint Analysis if you enable this feature for both inbound and outbound mail on the **BASIC > Spam Checking** page. In order to detect real-time spam fingerprints, Barracuda Real-Time Protection must be enabled on the **BASIC > Virus Checking** page.

Engineers at Barracuda Central work around the clock to identify new spam fingerprints which are then updated on all Barracuda Email Security Gateways through hourly Barracuda Energize Updates.

Intent Analysis

As for inbound mail, this feature is applicable for outbound mail, and block or quarantine actions can be specified accordingly on the **BASIC > Spam Checking** page.

Image Analysis

Fingerprint Analysis captures a significant percentage of images after they have been seen, while Image Analysis techniques protect against new image variants. The techniques detailed in Image Analysis (Inbound Mail) also apply to outbound messages. Image Analysis is configured on the **BASIC > Spam Checking** page.