Content Analysis Inbound

https://campus.barracuda.com/doc/3866700/

Custom Content Filters

The Barracuda Email Security Gateway enables administrators to set custom content filters based on the subject line, message headers, message body and attachment file content. In general, administrators do not need to set their own filters for the purposes of blocking spam, as these forms of rules are delivered to the Barracuda Email Security Gateway automatically through Barracuda Energize Updates. The online help for the **BLOCK/ACCEPT > Content Filtering** page includes a link to a Regular Expressions help page that covers expressions you can use for advanced filtering. HTML comments and tags embedded between characters in the HTML source of a message are also filtered.

You can specify actions to take with messages based on pre-made patterns in the subject line or message body. Credit card, Social Security numbers, privacy information such as driver's license numbers, phone numbers or expiration dates and HIPAA data can be automatically checked and acted upon by blocking, tagging or quarantining inbound messages.

Attachment Filtering

All messages, except those from whitelisted senders, go through attachment filtering. From the **BLOCK/ACCEPT > Attachment Filters** page you can choose to take certain actions with inbound and/or outbound messages if they contain attachments with certain filename patterns, file types, MIME types, or password protected archives. Actions you can take with inbound messages include *block* or *quarantine*. Actions you can take with outbound messages include *block, quarantine*, *encrypt* or *redirect.* You can elect to have a notification sent to the sender when an inbound or outbound message is blocked due to attachment content filtering. See the **ADVANCED > Bounce/NDR Settings** page to configure notifications.

The **BLOCK/ACCEPT > Attachment Filters** page provides a table of patterns you can use for specifying the above actions based on attachment filenames, or you can create your own filters.

The **Check Archives** feature can be selected along with any filter to search the contents of attached archives (zip, tar, etc.) and take one of the above actions with inbound or outbound messages based on filenames or types.\

Password Protected Archive Filtering

Use the **Password Protected Archive Filtering** feature to take action with messages with attachments that contain password protected (encrypted) archives.

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.

Attachment Filtering and the Message Log

Messages that are blocked due to attachment filtering will appear in the Message Log with the word *Attachment* and the filename in the **Reason** column. For example, if you created a filter on the **BLOCK/ACCEPT > Attachment Filters** page to block messages with attachments whose filenames match a pattern of **word***, the entry in the **Message Log** for such a blocked message would contain something like this in the **Reason** column:

Attachment (word_2010_xml.tgz)

where **word_2010_xml.tgz** is the attachment filename that caused the message to be blocked.

> The default maximum attachment size allowed by your Barracuda Email Security Gateway is 100 megabytes. If a message exceeds this size, the Barracuda Email Security Gateway rejects the message and the sending server notifies the sender that their message did not go through. Contact Barracuda Networks Technical Support to change this maximum.

Blocking Email by Country

Set tag, quarantine and block policies for specific character sets or regional spam settings using the **BLOCK/ACCEPT > Regional Settings** page. Here you can also choose to specifically allow messages based on valid Chinese or Japanese language content and enable compliance with PRC (People's Republic of China) requirements if your Barracuda Email Security Gateway resides in the PRC.

Fingerprint Analysis

A message "fingerprint" is based on commonly used message components (e.g., an image) across

many instances of spam. Fingerprint analysis is often as a useful mechanism to block future instances of spam once an early outbreak is identified. Spam fingerprints blocked based on a real-time check will display an '*' before "Fingerprint" in the Message Log. 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. Fingerprint Analysis is configured on the **BASIC > Spam Checking** page.

Intent Analysis

All spam messages have an "intent" to get a user to reply to an email, visit a web site or call a phone number. Intent analysis involves researching email addresses, web links and phone numbers embedded in email messages to determine whether they are associated with legitimate entities. Frequently, Intent Analysis is the defense layer that catches phishing attacks. The Barracuda Email Security Gateway features multiple forms of Intent Analysis:

- **Intent analysis** – Markers of intent, such as URLs, are extracted and compared against a database maintained by Barracuda Central, and then delivered to the Barracuda Email Security Gateway via hourly Barracuda Energize Updates. Intent can also be associated with general content categories, several of which are provided for Intent filtering.
- **Real-time intent analysis** – For new domain names that may come into use, Real-Time Intent Analysis involves performing DNS lookups against known URL blocklists.
- **Multilevel intent analysis** – Use of free web sites to redirect to known spammer web sites is a growing practice used by spammers to hide or obfuscate their identity from mail scanning techniques such as Intent Analysis. Multilevel Intent Analysis involves inspecting the results of web queries to URLs of well-known free web sites for redirections to known spammer sites. Intent Analysis is configured on the **BASIC > Spam Checking** page.

Image Analysis

Image spam represents about one third of all traffic on the Internet. While Fingerprint Analysis captures a significant percentage of images after they have been seen, the Barracuda Email Security Gateway also uses Image Analysis techniques which protect against new image variants. These techniques include:

- **Optical character recognition (OCR)** – Embedding text in images is a popular spamming practice to avoid text processing in anti-spam engines. OCR enables the Barracuda Email Security Gateway to analyze the text rendered inside the images.

- **Image processing** – To mitigate attempts by spammers to foil OCR through speckling, shading or color manipulation, the Barracuda Email Security Gateway also utilizes a number of lightweight image processing technologies to normalize the images prior to the OCR phase. More heavyweight image processing algorithms are utilized at Barracuda Central to quickly generate fingerprints that can be used by Barracuda Email Security Gateways to block messages.
- **Animated GIF analysis** – The Barracuda Email Security Gateway contains specialized algorithms for analyzing animated GIFs for suspect content.

Image Analysis is configured on the **BASIC > Spam Checking** page.