How to Configure Content Stripping, Grey Listing, and Blacklists

https://campus.barracuda.com/doc/43847175/

To manage the content that is forwarded by the mail gateway, you can configure blacklists and grey listing. You can also configure the mail gateway to strip specific types of content from mail.

In this article:

Configure Content Stripping

You can configure the mail gateway to strip the following content:

- **Attachments –** Strip specific attachment file types before forwarding mail to recipients. You can also exclude specific senders and recipients from having attachments stripped from their mail.
- **HTML Tags –** To protect your network from HTML email with annoying or potentially dangerous content, such as hyperlinks leading to fake websites and images with objectionable content, configure the mail gateway to remove HTML tags. As a result, links lose their function and images can no longer be loaded. Users are prevented from clicking on links unintentionally or thoughtlessly.
  Keep in mind that HTML tags are removed for incoming and outgoing email.
- **Received Lines –** Every SMTP server or relay registers itself within the mail header. These received lines may contain internal and confidential information about mail infrastructures. When the received lines are stripped, the number of "received" lines in the header stays the same but the content is replaced by dummy entries and thus no longer contains security critical information.
- **Barracuda Networks ID –** Remove the Barracuda Networks ID from the mail header of dispatched email. This can help conceal the identify of the mail gateway and decrease software traceability.

To configure content stripping, complete the following steps:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Mail-Gateway > Mail Gateway Settings**.
2. In the left menu, select **Content Adaptations**.
3. Click **Lock**.
4. Specify the content to be stripped. Follow the steps in the following table for the content that you want to be stripped from mail:

Task	Steps

To strip attachments:

1. In the **Attachment Stripping** section, select *yes* from the **Enable Attachment Stripping** list.
2. Next to **Advanced Attachment Options**, click **Set** or **Edit**.
3. Edit the attachment stripping settings. For more information on these settings, expand the following **Settings Overview** section:

Settings Overview

Setting	Description
Cut Whitelists	To exclude mail for certain senders and recipients from having attachments stripped, click **Set**. In the **Sender Whitelist** and **Recipient Whitelist** tables, add the email addresses and domain patterns for these senders and recipients. You can enter full addresses or wildcard characters (such as *user@barracuda.com*, *@barracuda.com*, and *barracuda.com*). The entries for the **Sender Whitelist** are processed before those in the **Recipient Whitelist**. An incoming email is first scanned for its sender. If the sender is in the whitelist, the email is forwarded with its attachments. If the sender is not in the whitelist, the email is scanned for its recipients. If the email is addressed to multiple recipients, it is only forwarded with its attachments if all of its recipients are listed in the **Recipient Whitelist**; otherwise, attachments are cut.
MIME-Type	In this table, add the MIME types of attachments that must be stripped. You can use wildcard characters. The following syntax applies: MIME-Type/MIME-Subtype For example: `*/*, application/*, application/activemessage` For an authoritative listing of all MIME types, see http://www.iana.org/assignments/media-types/. If wildcards are applicable, exclude specific subtypes from attachment stripping by adding them to the **MIME-Type Exceptions** table.
MIME-Type Exceptions	To exclude specific MIME subtypes from attachment stripping, add them to this table. You can use wildcard characters. The following syntax applies: MIME-Type/MIME-Subtype For example: `application/pdf, image/*`
Automatically Detect MIME-Type	It is recommended that you select **yes** to use the UNIX `file` command to detect MIME types automatically. To use the MIME type that is propagated by the sender's email client, select **no**.
File Extension Filter	In this table, add the file types of attachments that must be stripped. To add a file type is not listed, select the **Other** check box and enter the extension for the file type.
Message to Recipient	In this field, enter a message that informs recipients if file attachments have been cut from their mail. This message is inserted into the email before it is forwarded to the recipient.

4. Click **OK**.

To strip HTML tags:	1. In the **HTML Tag Removal** section, select *yes* from the **Remove HTML Tags** list. 2. To remove link tags, select *yes* from the **Remove HTML Link Tag** list. Links lose their function, but the string of the link itself remains unchanged. The linked destination can be viewed by copying the link from the email and pasting it into the address field of the browser. 3. To remove image source tags, select *yes* from the **Remove HTML Img Src Tag** list. Image source tags are altered so that they lose their function. Linked images will no longer be loaded from the servers they are placed on. Keep in mind that this function destroys the design of incoming and outgoing HTML email (such as newsletters).
To strip received lines:	1. In the **Misc** section, select **yes** from the **Strip Received Lines** list. 2. In the **Strip Received Lines Text** field, enter the text that replaces the original text that is stripped from the email header.
To remove the Barracuda Networks ID:	In the **Misc** section, select *yes* from the **Remove Barracuda Networks ID** list.

5. Click **Send Changes** and **Activate**.

Configure Grey Listing

Grey listing helps reduce SPAM by initially rejecting a message with an unknown sender-recipient pair. A rejection notice is sent to the mail server and the sender-recipient pair are placed on the grey list. The mail server is also told to try sending the mail again. A mail transfer agent (MTA) that has been correctly configured will attempt to resend the mail. The second delivery attempt is accepted and the email is delivered. Typically, SPAM is sent by non-RFC conforming servers that ignore error reports and do not try resending mail.

With grey listing, consider the following:

- Depending on the configuration of the sending MTAs, the email sender might be issued a report about the initial delivery failure.
- There is a slight delay in mail delivery because emails are initially rejected.
- Wanted emails may not be delivered if MTAs for the sender are not correctly configured. In this case, you can add the sender to the whitelist in the grey listing configuration.

To configure grey listing, complete the following steps:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Mail-Gateway > Mail Gateway Settings**.
2. In the left menu, select **Content Adaptations**.
3. Click **Lock**.
4. In the **Grey Listing** section, select *yes* from the **Enable Grey Listing** list.
5. Next to **Advanced Grey Listing Options**, click **Set** or **Edit**.
6. Edit the grey listing settings. For more information on these settings, expand the following **Settings Overview** section:
   Settings Overview

Setting	Description
Grey Listing Time (Min)	The length of time in minutes that must pass between the first and the second SMTP delivery attempt (default: *1*). Higher values increase the length of message delivery delay.
White List Peers	In this table, add the email addresses or domains for MTAs that are excluded from grey listing. You can also use wildcard characters. For example: `host.mailsrv.com, *.mailsrv.com, 172.16.1.` Do not enter network address ranges.
White List Senders	In this table, add the email addresses or domains for senders that are excluded from grey listing. You can use wildcard characters. For example, `*@barracuda.com`
Auto White List (Senders)	To automatically add senders to the white list after a successful mail transfer, select *yes*. To manage the number of senders in the white list, you can either edit the **Remove from White List after (d)** setting to specify the maximum number of days that senders can remain in the white list or manually delete senders. For more information on manually deleting senders, see How to Use the Grey Listing Tab.
Remove from Grey List after (h)	The maximum number of hours that sender-recipient pairs can remain in the grey list before they are removed (default: 24).
Remove from White List after (d)	The maximum number of days that sender-recipient pairs can remain in the white list after being automatically added (default: 30).
Daily Report Mail to	By default, a daily report about the grey list is sent to the postmaster. You can also send this report to other recipients or disable it: ◦ To specify another recipient for these daily reports, select the **Other** check box and enter the email address of the recipient. For multiple recipients, enter a space-delimited list of email addresses. ◦ To disable the daily reports, select **Nobody** from the **Daily Report Mail to** list.

7. Click **OK**.
8. Click **Send Changes** and **Activate**.

Configure Blacklists

To block certain hosts, subjects, sender, or recipients, add them to the blacklist.

> Blacklists are a static way of blocking unwanted mail and should not be used as a spam filter. If you want to configure a spam filter, see How to Configure the Spam Filter Service.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Mail-Gateway > Mail Gateway Settings**.
2. In the left menu, select **Content Adaptations**.
3. Click **Lock**.
4. In the **Blacklists** section, select **yes** from the **Enable Blacklist** list.
5. Next to **Blacklists**, click **Set** or **Edit**.
6. Add the hosts, subjects, sender, or recipients to the blacklists. For more information on the blacklists, expand the following **Blacklists Overview** section:
   Blacklists Overview

<table>
<tr><th>Blacklists</th><th>Description</th></tr>
<tr><td>Subject Blacklist | Sender Blacklist | Recipient Blacklist</td><td>In these tables, add phrases to block unwanted subjects, senders, and recipients. Emails that match the phrases are banned.
To ban subjects that are composed of multiple items including space characters, use the following case-insensitive syntax:
<table>
<tr><th>Punctuation</th><th>Description</th></tr>
<tr><td>?</td><td>Use a question mark to identify space.</td></tr>
<tr><td>*</td><td>Use an asterisk to identify an arbitrary number of phrases. Spaces can also be identified by an asterisk.</td></tr>
<tr><td>" "</td><td>Use quotation marks to identify a complete phrase.</td></tr>
</table>
For an explanation on how example phrases are interpretation, see the following table:
<table>
<tr><th>Character</th><th>Syntax of banned subject</th><th>Interpretation</th></tr>
<tr><td>your password</td><td>your password</td><td>The filter will be ignored, because there is no applicable rule.</td></tr>
<tr><td></td><td>"your?password"</td><td>All emails with the exact subject your password will be blocked.</td></tr>
<tr><td></td><td>"*your?password*"</td><td>All emails with your password being a part of the subject phrase will be blocked regardless of the other phrases’ content(s).</td></tr>
<tr><td></td><td>"*your*password*"</td><td>All emails with the words your and password in the given succession will be blocked regardless of other phrases’ contents before, between, or behind these two words.</td></tr>
</table></td></tr>
<tr><td>IP Blacklist</td><td>To block mail from specific hosts, add their IP addresses to this table.</td></tr>
</table>

7. Click **OK**.
8. Click **Send Changes** and **Activate**.

Continue with How to Configure Mail Gateway Service Limits.