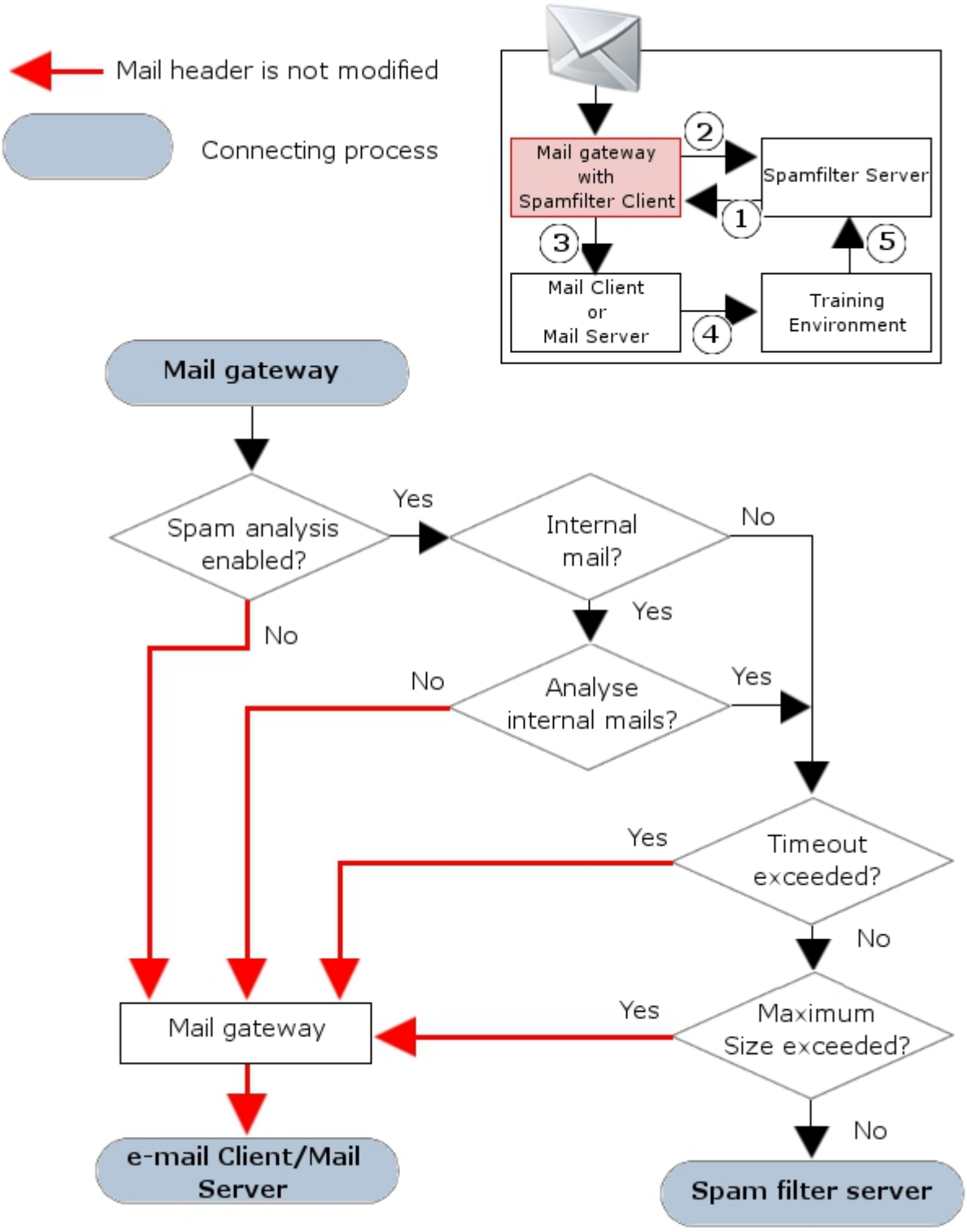
How to Configure Spam Filter Client Settings

https://campus.barracuda.com/doc/43847346/

The following article provides step-by-step information on how to configure the settings for the Barracuda NG Firewall´s Spam Filter Client. In order to be able to use this feature, make sure that a Spam Filter Service is introduced at your firewall as described in: How to Configure Services.

The SPAM Filter client’s work process involves the following:



Spam filter client configuration is done through the section **Spam Analysis** within the Mail Gateway settings (see: How to Configure Content Stripping, Grey Listing, and Blacklists).

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 Adaptions**.
3. Click **Lock**.
4. In the **Spam Detection** section, set the parameter **Enable Spam Analysis** to **yes**.
5. Click **Edit** to open the **Advanced Spam Options** window.
6. Set the appropriate values for the parameters explained in the sections below.
7. Click **OK**.
8. Click **Send Changes** and **Activate**.

Only Barracuda NG Firewall SPAM-Filter services may be used as spam engines.

MailGW Settings - Spam Analysis

Parameter	Description
Spam Analyzer IP	This IP address is the Bind IP of the SPAM Filter service (Bind or Additional IP, see below section **Configuring the Spam Filter Server**). Optionally, you may enter a DNS resolvable host name. The host name can be used to implement load balancing for high traffic scenarios.
Spam Analyzer Port	This value (default: **783**) must correspond with the port defined for the SPAM Filter service (Listening Port, see below section **Configuring the Spam Filter Server**).
Max. Size (MB)	This parameter defines the maximum size an e-mail may need to be processed by the SPAM Filter. If the e-mail exceeds this value (default: **1 MB**) it will not traverse the filter mechanism and will be delivered to its recipient without header modification (spam tag) instead.
Timeout (sec)	This parameter defines the maximum duration (default: **60 s**) it may take to analyze an e-mail. If the value is exceeded, the e-mail is delivered to its recipient without header modification (spam tag).
Analyze Internal Mails	When set to **yes** (default: **no**) mail traffic generated by internal mail domains is also classified. Analyzing of internal mail traffic may lead to high CPU load.
Deny Threshold	An e-mail is rejected when it exceeds the threshold configured here. The threshold is calculated from an e-mail's spam score (resulting from the testing sequences) multiplied by factor 100. To deactivate this parameter, enter a threshold of **0**.

Enable Domain Check	This field allows for checking of sender domains. The following options are available: • **None –** Sender domains are not checked for validity. • **MX –** Sender is only accepted if it is one of the domain's MX servers. • **Host-Domain –** Sender is only accepted if it is within the mail domain. For example, if the sending e-mail address is e.example@foo.com then the sending host has to be within domain foo.com. • **All-MX-Domains –** Sender has to be in a domain of the mail-domain MX servers. For example, if the sending e-mail address is e.example@foo.com and the MX servers of the domain foo.com are server1.foo.com and server1.backupfoo.com then the sending host has to be either in domain foo.com or backupfoo.com. Domain check failure results in one of the actions configured through parameter **Domain Action** (see next entry).
Domain Action	This field only has to be configured, if domain checking (see above) has been enabled. Domain check failure results in one of the following actions: • **logging –** The e-mail is delivered and a corresponding log entry is created. • **deny –** The e-mail is not delivered and a corresponding log entry is created.
Domain Whitelist	This field takes a list of trusted domains, which should be excluded from spam filtering. This list is consulted before the SPAM Filter is applied. Top-level and sub-domains may be defined (like barracuda.com and *.barracuda.com).

Continue with How to Configure the Spam Filter Service.

Figures

1. sf_flow.png