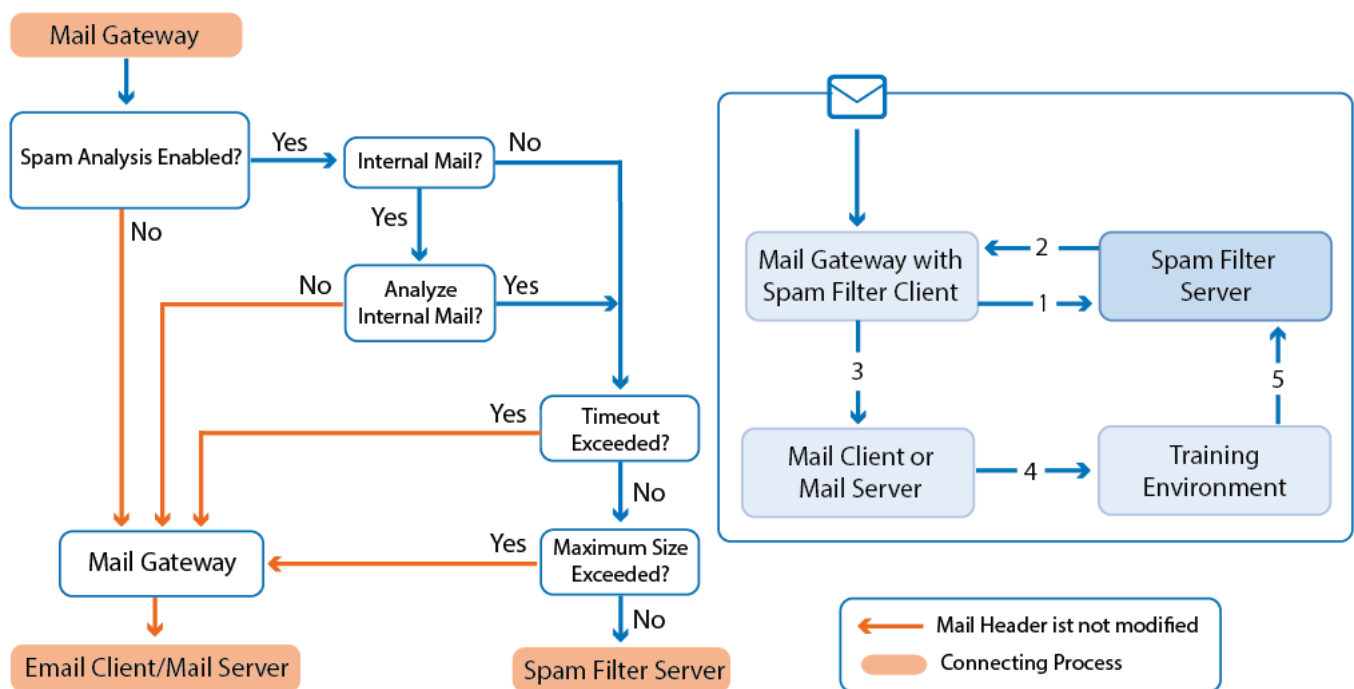


## How to Configure Spam Filter Client Settings

<https://campus.barracuda.com/doc/73719354/>

To configure the Spam Filter Client on a Barracuda CloudGen Firewall, a Spam Filter service must be introduced on your firewall. The firewall processes spam in combination with the Mail gateway service following these procedures:



### Configure the Spam Filter Client

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 **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 CloudGen Firewall Spam Filter services can be used as spam engines.

### MailGW Settings - Spam Analysis

Parameter	Description
<b>Spam Analyzer IP</b>	This IP address is the bind IP of the Spam Filter service. Optionally, enter a DNS-resolvable hostname. The hostname is used to implement load balancing for high traffic scenarios.
<b>Spam Analyzer Port</b>	This value (default: <b>783</b> ) must correspond with the port defined for the Spam Filter service
<b>Max. Size (MB)</b>	This parameter defines the maximum size an email can have to be processed by the Spam Filter. If the email exceeds this value (default: 1 MB), it will not traverse the filter. Instead, it will be delivered to its recipient without header modification (spam tag).
<b>Timeout (sec)</b>	This parameter defines the maximum allowed duration (default: 60 s) to analyze an email. If the value is exceeded, the email is delivered to its recipient without header modification (spam tag).
<b>Analyze Internal Mails</b>	When set to <b>yes</b> (default: no), mail traffic generated by internal mail domains is also classified. Analyzing internal mail traffic can lead to high CPU load.
<b>Deny Threshold</b>	An email is rejected when it exceeds this threshold. The threshold is calculated from an email's spam score (resulting from the testing sequences) multiplied by 100. To deactivate this parameter, enter a threshold of <b>0</b> .
<b>Enable Domain Check</b>	This field allows sender domains to be checked. The following options are available: <ul style="list-style-type: none"> <li>• <b>None</b> - Sender domains are not checked for validity.</li> <li>• <b>MX</b> - Sender is only accepted if it is one of the domain's MX servers.</li> <li>• <b>Host-Domain</b> - Sender is only accepted if it is within the mail domain. For example, if the sending email address is e.example@foo.com, the sending host must be within the domain foo.com.</li> <li>• <b>All-MX-Domains</b> - Sender must be in a domain of the mail domain MX servers. For example, if the sending email 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 must be either in the domain foo.com or backupfoo.com.</li> </ul> <b>Domain Check</b> failure results in one of the actions configured through the parameter <b>Domain Action</b> .
<b>Domain Action</b>	This action is carried out if the <b>Domain Check</b> fails: <ul style="list-style-type: none"> <li>• <b>logging</b> - The email is delivered and a corresponding log entry is created.</li> <li>• <b>deny</b> - The email is not delivered and a corresponding log entry is created.</li> </ul>
<b>Domain Whitelist</b>	This is 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 can be defined E.g., barracuda.com and *.barracuda.com To exclude emails from being checked for spam, apply the domain whitelists in the Spam Filter settings. For more information, see <a href="#">How to Configure the Spam Filter Service</a> .

## Next Step

---

Continue with [How to Configure the Spam Filter Service](#).

## Figures

1. fw\_spam\_filter\_client.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.