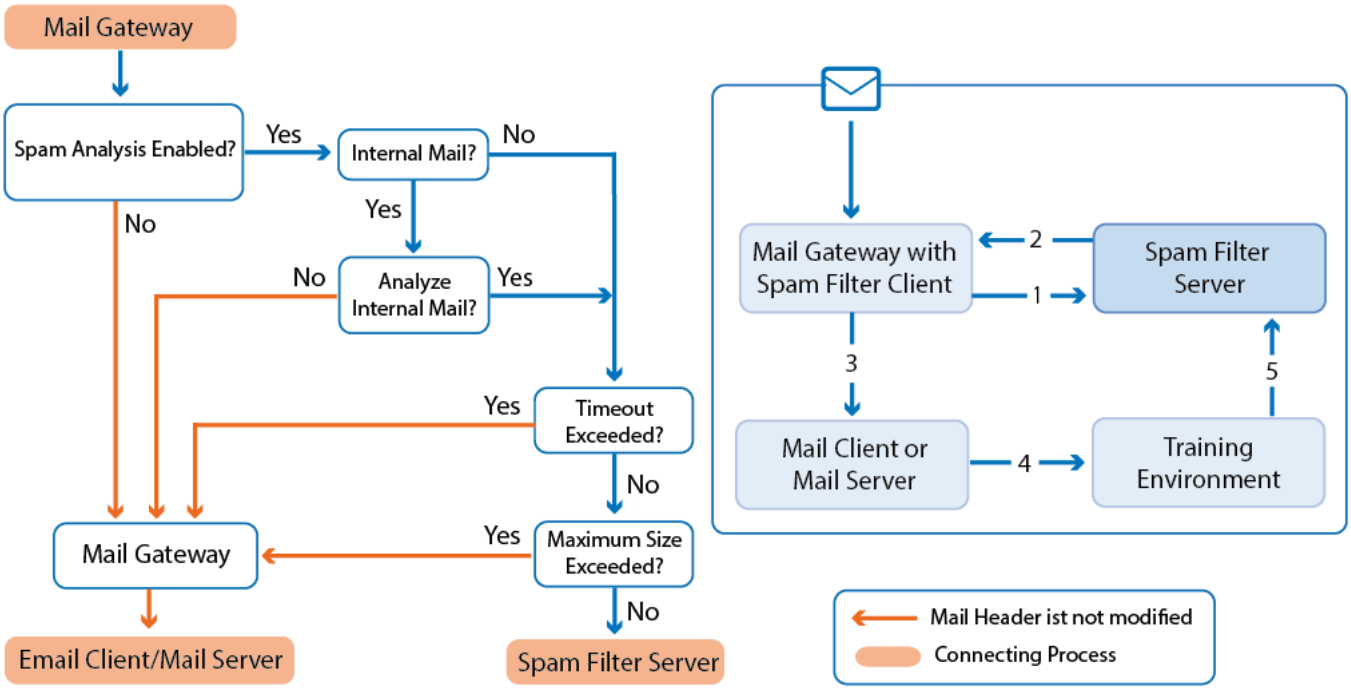
# How to Configure Spam Filter Client Settings

https://campus.barracuda.com/doc/53248806/

To configure the Spam Filter Client on a Barracuda NextGen Firewall F-Series, 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 NextGen Firewall F-Series Spam Filter services can 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. Optionally, enter a DNS-resolvable hostname. The hostname is 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 |
| **Max. Size (MB)** | 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). |
| **Timeout (sec)** | 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). |
| **Analyze Internal Mails** | When set to **yes** (default: no), mail traffic generated by internal mail domains is also classified.<br>Analyzing internal mail traffic can lead to high CPU load. |
| **Deny Threshold** | 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 **0**. |
| **Enable Domain Check** | This field allows sender domains to be checked. The following options are available:<br>• **None** – Sender domains are not checked for validity.<br>• **MX** – Sender is only accepted if it is one of the domain's MX servers.<br>• **Host-Domain** – 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.<br>• **All-MX-Domains** – 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.<br>**Domain Check** failure results in one of the actions configured through the parameter **Domain Action**. |
| **Domain Action** | This action is carried out if the **Domain Check** fails:<br>• **logging** – The email is delivered and a corresponding log entry is created.<br>• **deny** – The email is not delivered and a corresponding log entry is created. |
| **Domain Whitelist** | 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`<br>To exclude emails from being checked for spam, apply the domain whitelists in the Spam Filter settings. For more information, see How to Configure the Spam Filter Service. |

## Next Step

Continue with How to Configure the Spam Filter Service.

## Figures