Spam Filter

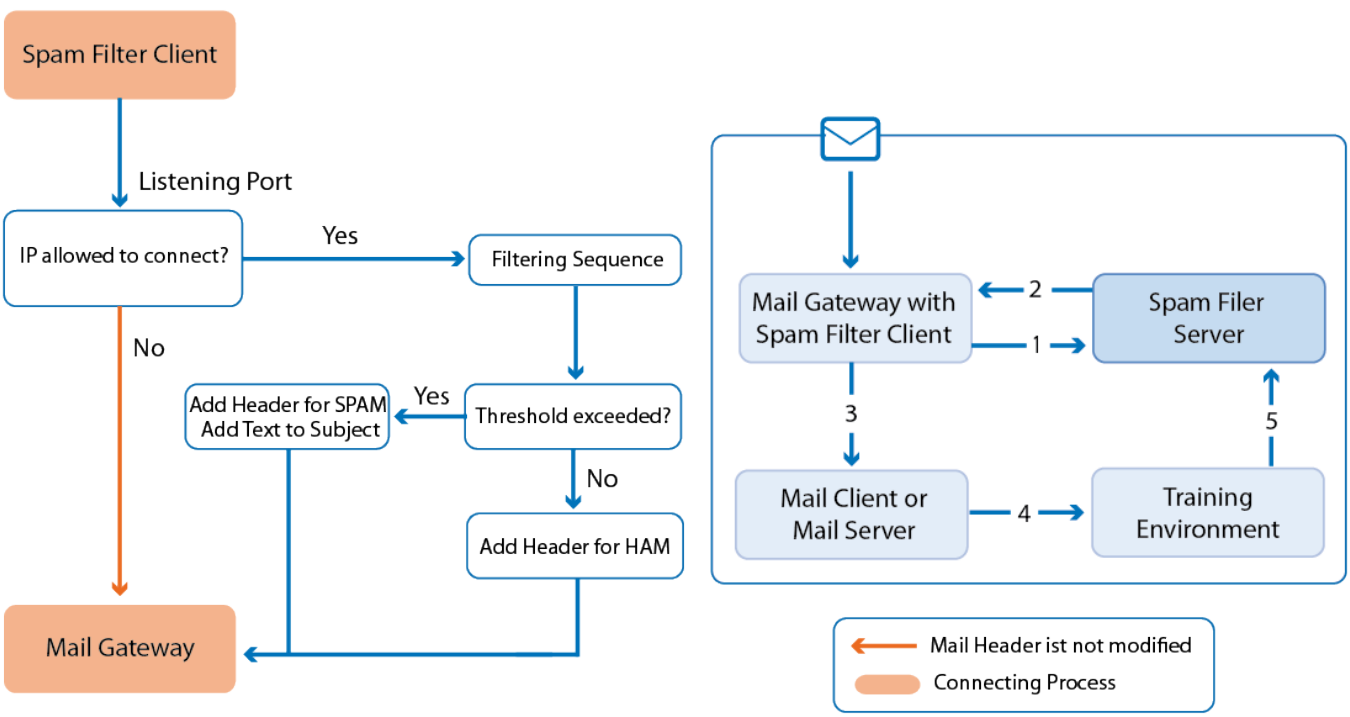
https://campus.barracuda.com/doc/46209110/

Barracuda NextGen Firewall F-Series provides spam filtering by placing the mail filter "SpamAssassin" at the disposal. "SpamAssassin" identifies spam by using mechanisms such as text analysis, Bayesian filtering, DNS blocklists, and collaborative filtering databases.

The SPAM Filter service is comprised of the following:

- Spam Filter Client
- Spam Filter Service
- (Optional) Training environment to improve email filtering

As illustrated by the following diagram and explained in the following sections, the components go through the following process to filter spam:



Step 1. The SPAM Filter Client Forwards Emails to the SPAM Filter Server

The Mail Gateway service pipes all mail traffic to the SPAM Filter server. The emails are then processed through SpamAssassin. If the SPAM Filter is not available, emails are delivered without filtering. SpamAssassin applies a variety of tests to determine whether or not an email is classified as spam. It examines the email's header and body locally against a configured ruleset and a Bayesian

filter. Each rule adds a value to the overall spam value of the email. If the score for the email exceeds a certain threshold (default: *5*), it is classified as spam.

The higher the score of an email, the higher the probability that it will be classified as spam. For more information about filtering mechanisms, see http://spamassassin.apache.org/tests_3_1_x.html.

The SPAM Filter then adds a tag to the mail header that indicates if the email is spam or ham:

Classification	Tag
Spam	X-SPAM-STATUS: **Yes**; X-SPAM-FLAG:**YES**
Ham	X-SPAM-STATUS: **No**

It also adds the test results to the email's body.

Example: Header of an email identified as spam

```
Received: from mailsrv.spammersnest.com ([1.2.3.4) by smtp.spammersnest.com
with Microsoft SMTPSVC(6.0.3790.1830); Fri, 24 Mar 2006 08:48:54 +0100
Received: from xxx ([x.x.x.x]) by xxx with xxx; 24 Mar 2006 08:48:09 -0100
Received: from xxx ([x.x.x.x]) by xxx with xxx; Fri, 24 Mar 2006 08:48:09
+0100 X-Message-Info: ZRCPB+dfk02+jvm+QG+760/7861938317196 Date: Fri, 24 Mar
2006 15:48:48 0800 Message-Id: From: "Geoff" <geoff572> To: Subject: [SPAM]
demehoqlola MIME-Version: 1.0 (produced by diqybdoxifut 0.4) Content-Type:
multipart/alternative; boundary="----------090708090808030606080206" X-phion-
id: 20060324-084808-02011-00 X-Spam-Prev-Subject: demehoqlola X-Spam-Flag:
YES X-Spam-Checker-Version: SpamAssassin 3.0.4 (2005-06-05) on
spamsrv.this.com X-Spam-Level: ** X-Spam-Status: Yes , score=2.6 required=2.0
tests=ALL_TRUSTED,BAYES_00,DATE_IN_FUTURE_06_12,HTML_MIME_NO_HTM
L_TAG,INVALID_DATE,MIME_HTML_ONLY,MIME_HTML_ONLY_MULTI,X_MESSAGE _INFO
autolearn=no version=3.0.4 X-Spam-Report: * 0.2 INVALID_DATE Invalid Date:
header (not RFC 2822)* 4.2 X_MESSAGE_INFO Bulk email fingerprint (X-Message-
Info) found* 1.3 DATE_IN_FUTURE_06_12 Date: is 6 to 12 hours after Received:
date* -3.3 ALL_TRUSTED Did not pass through any untrusted hosts* -2.6
BAYES_00 BODY: Bayesian spam probability is 0 to 1 %* [score: 0.0042]* 0.2
MIME_HTML_ONLY BODY: Message only has text/html MIME parts* 0.1
HTML_MIME_NO_HTML_TAG HTML-only message, but there is no HTML tag* 2.4
MIME_HTML_ONLY_MULTI Multipart message only has text/html MIME parts X-
AntiVirus: checked by AntiVir MailGate (version: 2.0.3-25; AVE: 6.33.1.0;
VDF: 6.33.1.1; host: spamsrv.this.com) Return-Path: geoff572@spamdomain.net
X-OriginalArrivalTime: 24 Mar 2006 07:48:54.0566 (UTC)
FILETIME=[664AD460:01C64F17] X-TM-AS-Product-Ver:
```

```
SMEX-7.0.0.1345-3.52.1006-14342.000 X-TM-AS-Result: No-3.150000-8.000000-31
X-UIDL: AAQMd8AAAAQwBNsx5nZbMWkZBBoOyqFh TO: spam@this.com CC: BCC:
```

Step 2. The SPAM Filter Server Returns the Email to the Mail Gateway

After the email has been classified as spam or ham, it is returned to the mail gateway for further processing.

Step 3. The Mail Gateway Forwards Mail to the Email Client/Mail Server

Email clients may use the contents of the supplemented mail header to sort emails. For example, the additional information in the email header may be used to automate the forwarding of spam to a spam directory.

> Because emails may be incorrectly classified, it is not recommended that you automatically forward spam into the trash bin without verification. Instead, it is recommended that you set up a training environment to help improve the filtering mechanism.

Step 4. Improve Spam Filtering via the Training Environment

Because spam filtering is based on statistics, emails may be tagged incorrectly. To minimize the risk for such incidents, you can set up a training environment with a mail server to sort misclassified mail into three mailboxes:

- SPAM - Contains spam that was delivered and not tagged.
- HAM - Contains mail that was incorrectly tagged as spam.
- FORGET - Contains mail that should not be tagged as spam or ham.

Step 5. Spam Filter Server Update

If you set up a training environment, SpamAssassin regularly collects and processes the mail from the SPAM, HAM, and FORGET mailboxes to improve its filter mechanisms.

Figures

1. fw_spam_filter.png