

BitDefender AntiSpam for Mail Servers (Win SMTP Proxy)

QUICK START

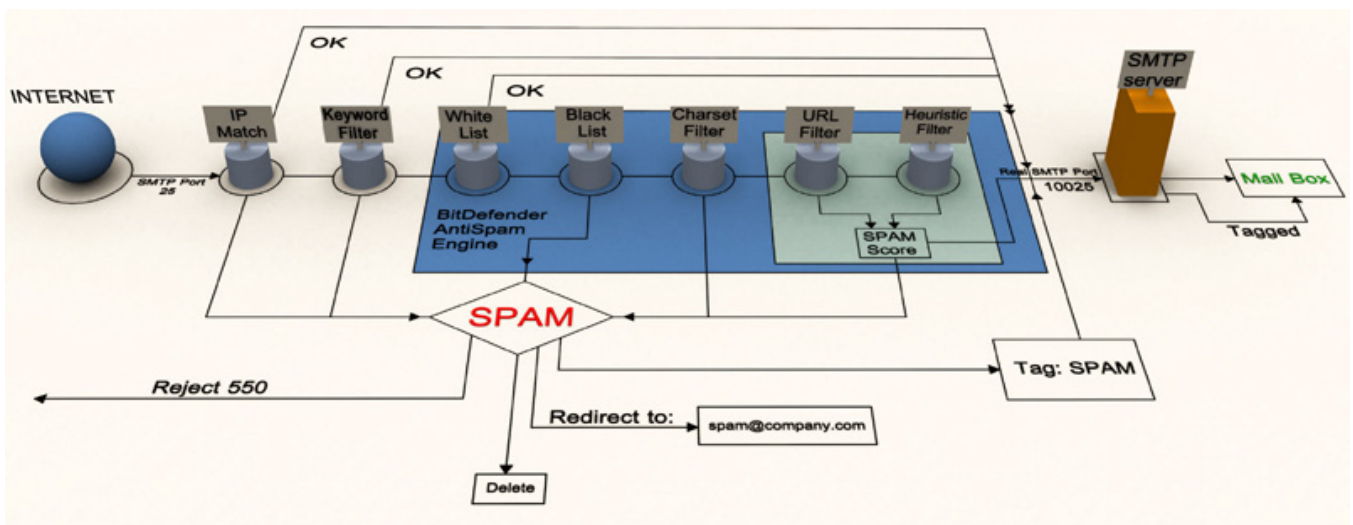


How does it work?

As lost time and bandwidth grow to be more and more of a problem, companies are finding it difficult to deal with the problem of spam. To help with this issue, BitDefender Labs designed the **BitDefender AntiSpam** module, an advanced spam filtering solution that integrates with the majority of existing e-mail platforms.

BitDefender AntiSpam (Win SMTP Proxy) checks every incoming & outgoing e-mail message and attaches a spam score. If the spam score is greater than or equal to the spam threshold, then the message is marked as spam. Otherwise, it's marked as non-spam.

For complete protection, **BitDefender AntiSpam** can be combined with any of the BitDefender Antivirus solutions for Mail Servers (BitDefender Antivirus - Win SMTP Proxy, BitDefender for Exchange 5.5 / 2000, BitDefender for Lotus Domino). It is also compatible with Enterprise Manager, which offers centralized management for the BitDefender products.



IP Match

Spammers often try to "spoof" the sender's e-mail address to make the email appear as if it is being sent by someone in your domain. To prevent this, enter a specific e-mail address to a specific IP address.

If the message appears to be from a domain that you have specified in your **IP Match** setting (such as your own company domain), BitDefender checks to see if the IP address of the sender matches the IP address entered for the specified domain. If the sender's domain address, match the IP address, the message will be delivered directly to the mail server. Otherwise the message will be tagged as SPAM.

Keyword filter

A keyword filter is implemented "before" the AntiSpam filter. Relevant categories are message subject, headers and body. A set of explicit allow / don't allow rules must be defined. If and only if a particular piece of e-mail passes through the keyword filter, it reaches the AntiSpam filter.

White list / Black list

Most people communicate regularly to a group of people or even receive messages from companies or organizations in the same domain. By using **White/Black lists**, the admin can set a list of trusted and un-trusted addresses from which to respectively "always accept" or "always reject" e-mail messages.

We recommend that you add the trusted addresses to the **White List**. **BitDefender** does not block messages from those on the list; therefore, adding them helps ensure that legitimate messages get through.

Charset filter

The **Charset filter** helps you block all the e-mail messages written in Cyrillic and / or Asian charsets.

URL filter

Most of the spam messages contain links to various web locations (which contain more advertising and the possibility to buy things, usually). **BitDefender** has a database, which contains links to these kinds of sites.

Every URL link in an e-mail will be checked against the URL database. If it will be found, +45 will be added to the spam score.

Heuristic filter

BitDefender checks all the message components against many rules, (i.e. not only the header but also the message body in either HTML or text format), using the **Heuristic filter**. Each rule is given a numerical value and the aggregate of these values is an overall spam score that ranges from 0-100. The overall spam score is measured against the desired level of spam sensitivity (threshold), and a decision is made whether the message is spam or is valid.

Note

The techniques presented above - **IP Match**, **Keyword filter**, **White list / Black list**, **Charset filter**, **URL filter** and **Heuristic filter** - are used in conjunction by the **BitDefender AntiSpam** filter, to keep unwanted e-mail out of your organization.

FULLY CONFIGURABLE REACTIONS

- The e-mail messages tagged as spam can be sent to a valid, admin-set address, for periodic checking.
- The score returned by the AntiSpam library can be appended to the e-mail subject line. This is only done to e-mail, which exceeds the spam threshold.
- An attribute indicative of confidence level can be added to the header for all the messages (spam or non-spam).
- The e-mail messages tagged as spam can be rejected (SMTP error 550) or deleted.

SYSTEM REQUIREMENTS

- Minimum Processor: Pentium II 400MHz
- Minimum hard disk space: 20MB (50 MB Recommended)
- Minimum RAM Memory: 128MB
- Operating system: Windows NT 4.0 -SP6/2000/XP/2003 Server; IE 4.0 (+)

Best practices

1. After the installation process is over, please register the product.
2. You must specify the proxy settings for the SMTP server. Access the **AntiSpam** module (**SMTP** section) and introduce the proxy settings.
3. In the same window you must type the local domain (in order to receive all the e-mail messages) and the network address (in order to send all the outgoing e-mail messages from that address through proxy). For local domain you must click the **Add e-mail Domain** button and type in it. For network address you must click the **Add Net Domain** button and type in the network address and the mask.
4. Select the action to be taken on spam messages. Enter the **AntiSpam** section and select the desired action: redirect, reject, delete or ignore (no action). For redirect and ignore you can configure BitDefender to modify the subject.
5. In the same window, select the **Add header** check box. The result is that the header of all the messages (spam or not) will be modified.



Note

If you receive an e-mail that you think is spam, but BitDefender didn't tag it you can check the spam score in the e-mail properties.

6. Verify that BitDefender is working with the GTUBE test. The test consists in entering the `XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X` line in the body of an e-mail. BitDefender must tag as spam any message that contains this string.



The string must be reproduced on a single line.

7. Configure the filters: **IP Match**, **Charset filter**, **Keyword filter**, **White list** and **Black list**.
8. If an unexpected situation appears, there is the possibility of sending alarm messages by e-mail or by net send. Access the **Mail Notification** section or the **NetSend Notification** section in order to configure BitDefender to send these notifications.



Note

Examples of unexpected situations: license expiration, protection disabled, errors in client - server communication, errors while starting BitDefender AntiSpam and so on.

9. Configure the update. Enter the **BitDefender Update** section and if you are using a proxy check **Use Proxy** and type in the settings. You can change the update interval (the default interval is 8 hours).