

Introduction to the Barracuda Spam and Virus Firewall

Barracuda is a Spam/Virus *firewall*. The solution intercepts email before it hits the mail server and your email box. As viruses and spam techniques change over time, Barracuda adapts to new techniques used by spammers. Barracuda offers a number of benefits to you. First, your valuable time is conserved when you don't have to download and then manually filter through your email. This is especially beneficial for our dialup customers. Next, the annoyance of spam is greatly reduced. The Barracuda solution will eliminate almost all of your spam once you have trained it.

Barracuda isn't only an effective spam solution, however. It also intercepts and quarantines the latest Email viruses and trojans. While this won't guarantee that your computer will not contract a virus, it reduces the likelihood significantly.

Since Barracuda is such a robust solution for spam and virus filtering, it will require a change in thought process about how you interact with your email to reduce spam and viruses. For most users, the following pages of documentation may not be necessary, as the standard settings in Barracuda should eliminate almost all the spam and viruses you receive through email. If you wish to tweak settings, you will need to read these instructions to learn how to interact with Barracuda.

A few things have changed from the old spam filtering system. Based on user preferences, which you can configure via the interface, a number of actions can be taken on email. The first action is called "Tag" and it works much like the old spam filter whereby it puts a "tag" in the e-mail messages subject line indicating that the message is potentially spam. An example is [SPAM]. You can then setup your email client to filter these into a separate folder.

The second filtering option is "Quarantine". Your account in the spam filter system has an associated "quarantine" box, which is a holding area for suspected spam. You able to log into the spam filter's web interface and review e-mail that is suspected of being spam and has been placed in the quarantine box. This gives you some oversight into the spam filter's actions. Over time the filter will learn from these actions and become more accurate you.

The third option is an outright "Block" which does just like it sounds. At this point the filter will just delete the message and take no further action on it. The intended recipient will never see the message and won't receive notification of it being deleted.

See below to further explore how to configure Barracuda for your particular needs. Once again, however, most users can ignore the advanced configuration options of Barracuda and enjoy the benefits of automated spam and virus filtering.

Using the Barracuda Spam Firewall to Filter Your Emails

This chapter describes how end users interact with the Barracuda Spam Firewall to check their quarantined messages, classify messages as spam and not spam, and modify their user preferences. This chapter contains the following topics:

- Receiving Messages from the Barracuda Spam Firewall in the next section.
- Using the Quarantine Interface.
- Changing your User Preferences.
- Using the Microsoft Outlook Plugin

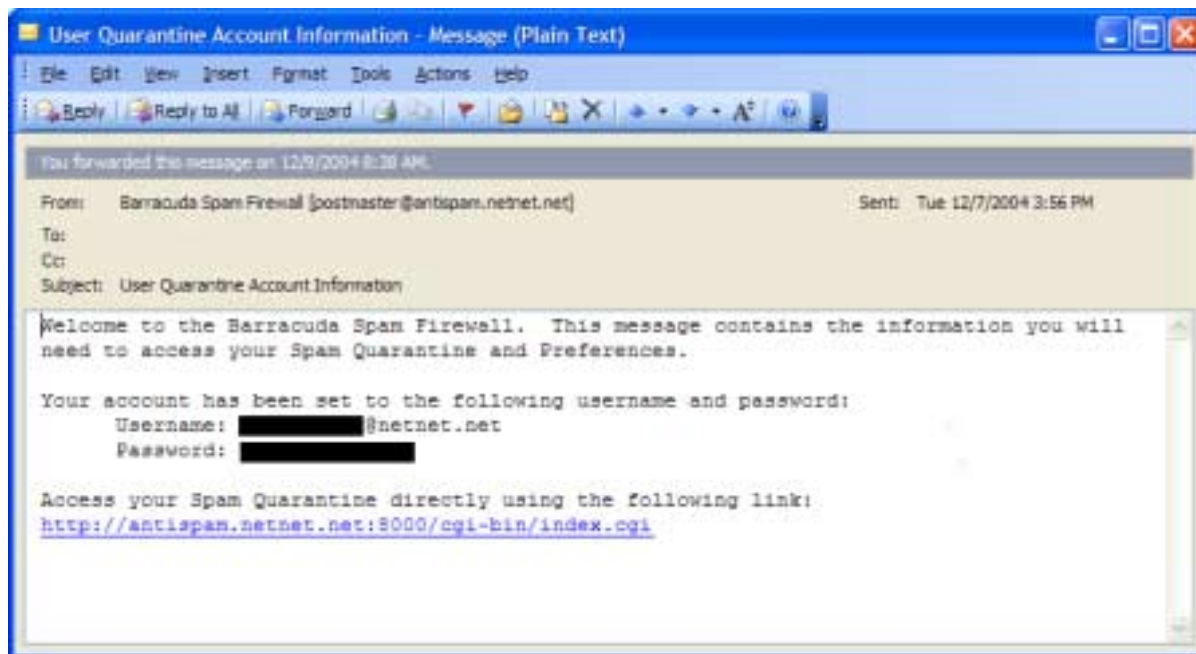
Receiving Messages from the Barracuda Spam Firewall

The Barracuda Spam Firewall sends the following two types of messages to end users:

- Greeting Message
- SPAM Quarantine Summary Report

Greeting Message

The first time the Barracuda Spam Firewall quarantines an email intended for you, the system sends you a greeting message with a subject line of “User Quarantine Account Information”. The greeting message contains the following information:



The Barracuda Spam Firewall automatically provides your login information (username and password) and the link to access the quarantine interface. You should save this email because future messages from the system do not contain your login information.

Quarantine Summary Report

The Barracuda Spam Firewall sends you a daily quarantine summary report so you can view


the quarantined messages you did not receive. From the quarantine summary report you can also add messages to your whitelist, delete messages, and have messages delivered to your inbox.

The following figure shows an example of a quarantine summary report.

Click to access the Quarantine interface to set preferences and classify messages

Select to deliver, whitelist or delete quarantined messages

From: Barracuda Spam Firewall [support@barracudanetworks.com] Sent: Tue 1/13/13
To: nguyen@affinitypath.com
Cc:
Subject: Daily Spam Quarantine Summary

 **Spam Quarantine Summary**


Dear **nguyen@affinitypath.com**, this is your daily quarantine summary from the Barracuda Spam Firewall.

You have **3** messages in your spam quarantine inbox.

- Click on the **Deliver** link to have a message delivered to your mailbox.
- Click on the **Whitelist** link to have a message delivered to your mailbox and whitelist the sender so that messages will no longer be quarantined.
- Click the **Delete** link to have the message deleted from your quarantine (message will be automatically for spam learning)

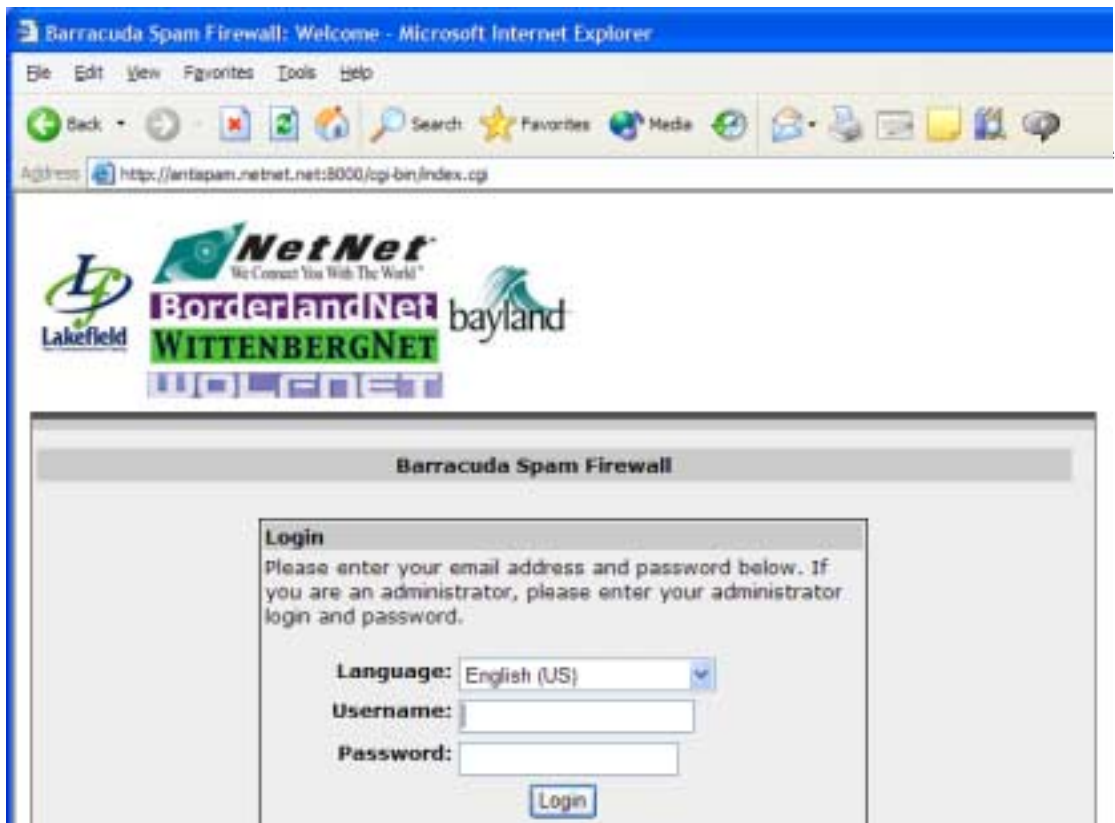
Date	From	Subject	Actions
01/12 13:01	"Khoa Nguyen" <khoa_barracu...>	welcome to paris you 1	Deliver Whitelist Delete
01/07 08:26	Peter Salenger <petesaleng@...>	hi test zip	Deliver Whitelist Delete
01/08 11:04	"Khoa Nguyen" <khoa_barracu...>	welcome to paris you 1	Deliver Whitelist Delete

To view your entire quarantine inbox or manage your preferences, [click here](#).

Spam/Virus Protection By 

Using the Quarantine Interface

At the end of every quarantine summary report is a link to the quarantine interface where you can set additional preferences and classify messages as spam and not spam.



2. Enter your username and password, and click **Login**.

Your login information resides in the greeting message sent to you from the Barracuda Spam Firewall.

Managing your Quarantine Inbox

After logging into the quarantine interface, select the QUARANTINE INBOX tab to view a list of your quarantined messages. When you first start using the quarantine interface, you should view this list on a daily basis and classify as many messages as you can.

The Barracuda Spam Firewall has a learning engine that learns how to deal with future messages based on the ones you classify as spam and not spam. The learning engine becomes more effective over time as you teach the system how to classify messages and as you set up rules based on your whitelist and blacklist.

Clicking on an email displays the message.

The following table describes the actions you can perform from this page.

Action	Description
Deliver	<p>Delivers the selected message to your standard email inbox.</p> <p><i>Note: If you want to classify a message or add it to your whitelist, make sure to do so before delivering the message to your inbox. Once the Barracuda Spam Firewall delivers a message, it is removed from the quarantine list.</i></p>
Whitelist	<p>Adds the selected message to your whitelist so all future emails from this sender are not quarantined unless the message contains a virus or banned file type.</p> <p>The Barracuda Spam Firewall adds the sending e-mail address exactly as it appears in the message to your personal whitelist.</p> <p>Note that some commercial mailings may come from one of several servers such as "mail3.abcbank.com", and a subsequent message may come from "mail2.abcbank.com". See the section on managing your whitelists and blacklists for tips on specifying whitelists with greater effectiveness.</p>
Delete	<p>Deletes the selected message from your quarantine list. The main reason to delete messages is to help you keep track of which quarantine messages you have reviewed.</p> <p>You cannot recover messages you have deleted.</p>
Classify as Not Spam	<p>Classifies the selected message as not spam.</p> <p><i>Note: Some bulk commercial mail may be considered useful by some users and spam by others. For this reason, classifying such messages may not be very effective because users may counteract each others' classification. Instead of classifying bulk commercial mail, it may be more effective to add it to your whitelist (if you wish to receive such messages) or blacklist (if you prefer not to receive them).</i></p>
Classify as Spam	<p>Classifies the selected message as spam.</p>

Changing your User Preferences

After logging into the quarantine interface, select the PREFERENCES tab to change your account password, modify your quarantine and spam settings, and manage your whitelist and blacklist.

Changing your Account Password

To change your account password, do one of the following:

- On the quarantine interface login page, click **Create New Password**, or
- After logging into the quarantine interface, go to PREFERENCES-->Password.

In the provided fields, enter your existing password and enter your new password twice. Click **Save Changes** when finished.

Note: Changing your password breaks the links in your existing quarantine summary reports so you cannot delete, deliver, or whitelist messages from those reports. New quarantine summary reports contain updated links that you can use the same as before.

Changing Your Quarantine Settings

The following table describes the quarantine settings you can change from the PREFERENCES-->Quarantine Settings page.

Quarantine Setting	Description
Enable Quarantine	Whether the Barracuda Spam Firewall quarantines your messages. If you select Yes , the Barracuda Spam Firewall does not deliver quarantined messages to your general email inbox, but you can view these messages from the quarantine interface and quarantine summary reports. If you select No , all messages that would have been quarantined for you are delivered to your general email inbox with the subject line prefixed with "[QUAR]:". The Barracuda Spam Firewall administrator can modify this prefix.
Notification Interval	The frequency the Barracuda Spam Firewall sends you quarantine summary reports. The default is daily. The Barracuda Spam Firewall only sends quarantine summary reports when one or more of your emails have been quarantined. If you select Never , you can still view your quarantined messages from the quarantine interface, but you will not receive quarantine summary reports.
Notification Address	The email address the Barracuda Spam Firewall should use to deliver your quarantine summary report. Leave this field blank to use the email address associated with your user account.

Enabling and Disabling Spam Scanning of your Email

If you do not want the Barracuda Spam Firewall scanning your emails for spam content, you can disable spam filtering from the [PREFERENCES-->Spam Settings](#) page. From this page you can also change the default spam scoring levels that determine when your emails are tagged, quarantined or blocked.

When the Barracuda Spam Firewall receives an email for you, it scores the message for its spam probability. This score ranges from 0 (definitely not spam) to 10 or higher (definitely spam). Based on this score, the Barracuda Spam Firewall either allows, quarantines, or blocks the message.

A setting of 10 for any setting disables that option.

Setting	Description
Spam Filter Enable/Disable	
Enable Spam Filtering	Select Yes for the Barracuda Spam Firewall to scan your emails for spam. Select No to have all your messages delivered to you without being scanned for spam.
Spam Scoring	
Use System Defaults	Select Yes to use the default scoring levels. To configure the scoring levels yourself, select No and make the desired changes in the Spam Scoring Levels section described below.
Spam Scoring Levels	
Tag score	Messages with a score above this threshold, but below the quarantine threshold, are delivered to you with the word [BULK] added to the subject line. Any message with a score below this setting is automatically allowed. The default value is 2.5.
Quarantine score	Messages with a score above this threshold, but below the block threshold, are forwarded to your quarantine mailbox. The default setting is 10 (quarantine disabled). To enable the quarantine feature, this setting must have a value lower than the block threshold.
Block score	Messages with a score above this threshold are not delivered to your inbox. Depending on how the system is configured, the Barracuda Spam Firewall may notify you and the sender that a blocked message could not be delivered. The default value is 9.

Adding Email Addresses and Domains to Your Whitelist and Blacklist

The [PREFERENCES-->Whitelist/Blacklist](#) page lets you specify email addresses and domains from which you do or do not want to receive emails.

List Type	Description
Whitelist	A list of e-mail addresses or domains from which you always wish to receive messages. The only time the Barracuda Spam Firewall filters a message from someone on your whitelist is when the message contains a virus or a disallowed attachment file extension.
Blacklist	A list of senders from whom you never want to receive messages. The Barracuda Spam Firewall immediately discards messages from senders on your blacklist. These messages are not tagged or quarantined and cannot be recovered. The sender does not receive a notice that the message was deleted, and neither do you.

To whitelist or blacklist senders, follow these steps:

1. Go to the PREFERENCES-->Whitelist/Blacklist page.

A list of your existing whitelisted and blacklisted addresses appears on this page.

2. To delete a whitelist or a blacklist entry, click the trash can icon next to the address.
3. To add an entry, type an e-mail address into the appropriate field, and click the corresponding **Add** button.

Tips on specifying addresses

When adding addresses to your whitelist and blacklist, note the following tips:

- If you enter a full email address, such as *john.doe@yahoo.com*, just that user is specified. If you enter just a domain, such as *yahoo.com*, all users in that domain are specified.
- If you enter a domain such as *barracudanetworks.com*, all subdomains are also included, such as *support.barracudanetworks.com* and *test.barracudanetworks.com*.
- Mass mailings often come from domains that do not resemble the company's web site name. For example, you may want to receive mailings from *historybookclub.com*, but you will find that this site sends out its mailing from the domain *hbcfyi.com*. Examine the From: address of an actual mailing that you are trying to whitelist or blacklist to determine what to enter.

Using the Microsoft Outlook Plugin

What is the Barracuda MS Outlook Plugin?

The Barracuda MS Outlook Plugin is a plugin for the Windows versions of Outlook. It requires Windows 98/2000/NT/XP. The plugin allows you to classify messages as spam or not-spam right from your desktop. This classification trains the learning filter and results in higher accuracy for targeting spam for future filtering.

Installing the Plugin

To install the plugin, click on the link on the main Barracuda login page.

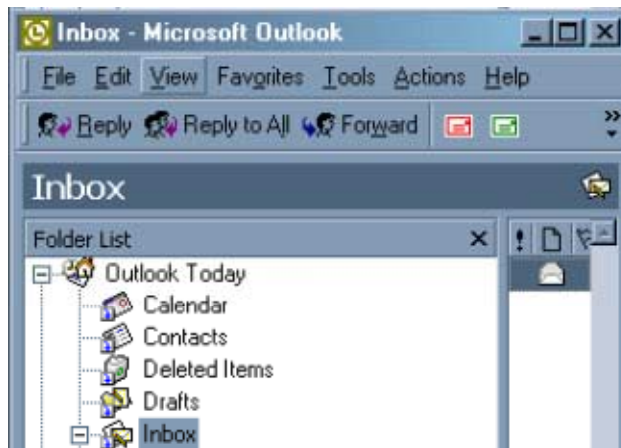


Using the Plugin

Once installed, the Plugin makes itself available to you through the toolbar inside MS Outlook. Two icons are provided that perform the necessary classification functionality: a red envelope to classify messages as spam, and a green envelope to classify messages as not-spam.

To use the plugin, select one or more items from the message window and click on the spam/not-spam icon to submit the messages to the Barracuda Spam Firewall for classification.

For convenience, the toolbar icons are also provided when a mail message is opened in a new window for viewing. If desired, the message can be classified immediately from that window.



Also note, learning is only effective when the differences between spam and not-spam are known to the system. Therefore it is important to make sure that both types of messages are classified from your desktop. This plugin is designed to make that classification process as easy as possible. However, it is up to you to make sure the items they classify from the plugin are really considered spam or not-spam as it will affect the scoring of future messages coming onto the system for you.