

# **Gordon State College**

## **Spam Firewall**



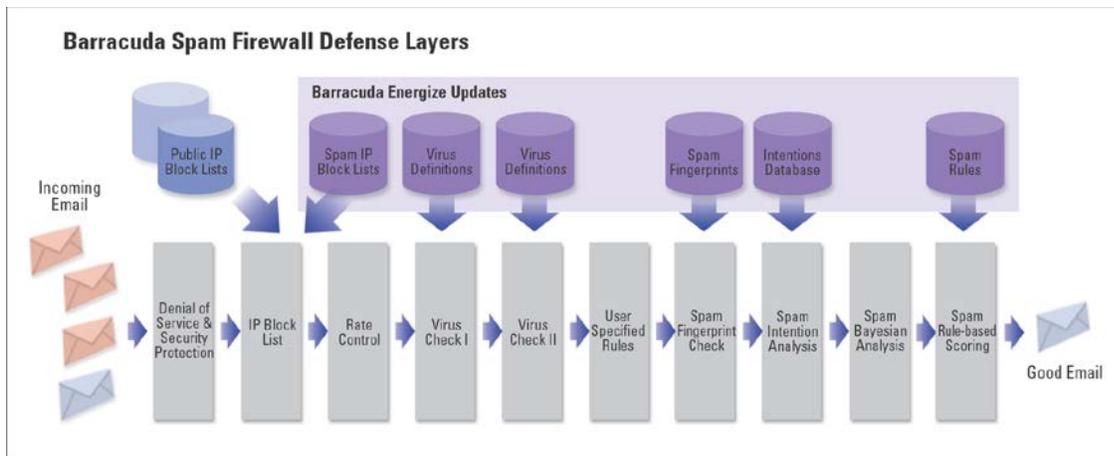
**User Guide**

## Overview

The Barracuda Spam Firewall is an integrated hardware and software solution that provides powerful and scalable spam and virus-blocking capabilities that do not impede the performance of your email servers. The system has no per-user license fee and can be scaled to support tens of thousands of active email users. Using the Web-based administration interface, you can configure up to ten defense layers that protect your users from spam and viruses. The ten defense layers are:

- Denial of service and security protection
- IP block list
- Rate control
- Virus check with archive decompression
- Proprietary virus check
- User-specified rules
- Spam fingerprint check
- Intention analysis
- Bayesian analysis
- Rule-based spam scoring

The following figure shows each of these defense layers in action:



## How Spam is scored

The Barracuda Spam Firewall scrutinizes all the characteristics of a message and uses a complex system of scores to determine whether a message is spam. When an email reaches the spam scoring filter, the Barracuda Spam Firewall assigns scores to all the properties of the message. For example, the Barracuda Spam Firewall scrutinizes:

- A message's header and subject line for offensive characters or words
- The percentage of HTML in the message
- Whether a message contains an "unsubscribe" link

These properties (along with many others) help the Barracuda Spam Firewall determine the spam score for a message that is displayed on the Message Log page of the administration interface. Energize Updates keeps the spam rules and scores up-to-date so the Barracuda Spam Firewall can quickly counteract the latest techniques used by spammers.

## What is quarantined email

Quarantined email is sent to a special user mailbox on the Barracuda Spam Firewall. With the exception of viruses, email messages are stored in their entirety, and can be retrieved should the need arise. User quarantined email is stored on the Barracuda Spam Firewall itself.

## Quarantined email report

The Barracuda Spam Firewall sends you the following two types of messages:

- 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:

*Welcome to the Gordon State College Spam Firewall. This message contains the information you will need to access your Spam Quarantine and Preferences*

*Your account has been set to the following username:*

*Username: <your email address>*

*Access your Spam Quarantine directly using the following link:*

*<https://condor.gordonstate.edu>*

Your login information to the Barracuda Spam Firewall is the same username and password you use to access the Gordon State College network.

### ***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 your quarantine interface to set preferences and classify messages

Select to deliver, whitelist or delete quarantined messages

**Gordon College SPAM Firewall**

Account: **britt@gdn.edu**

This is your quarantine summary from the Gordon College SPAM Firewall.

You have **2** 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 his/her messages will no longer be quarantined.
- Click the **Delete** link to have the message deleted from your quarantine.

Time Received	From	Subject	Actions
01/25/07 15:59:13	blifsey@mindspring.com	qttest 6	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
01/25/07 15:50:19	blifsey@mindspring.com	qttest 5	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>

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

Spam/Virus Protection By

## Accessing quarantined email

At the end of every quarantine summary report is a link to the quarantine interface where you can classify messages as spam/not spam and specify email addresses and domains from which you do or do not want to receive emails. You can also access the quarantine interface at the URL <https://condor.gordonstate.edu>.

## Logging into the Quarantine Interface

To log into your quarantine interface:

1. Click the link provided at the bottom of the Quarantine Summary Report (displayed above).  
Result: Login page appears.
2. Enter your username and password, and click Login.

Your login information to the Barracuda Spam Firewall is the same username and password you use to access the Gordon State College network.

## 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.

<b>Action</b>	<b>Description</b>
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 your 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 attachment type.</p> <p>The Barracuda Spam Firewall adds the sending email address exactly as it appears in the message to your personal whitelist.</p> <p><i>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.</i></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 email may be considered useful by some users and spam by others. Instead of classifying bulk commercial email, 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 your quarantine interface, you can use the PREFERENCES tab to manage your whitelist and blacklist.

### ***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	The list of email addresses or domains from which you always wish to receive messages. The only time the Barracuda Spam Firewall blocks a message from someone on your whitelist is when the message contains a virus or a disallowed attachment file extension.
Blacklist	The 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. The only time a blacklisted email address is delivered is if the same email address also appears in your whitelist

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 email address or domain 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 johndoe@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.