

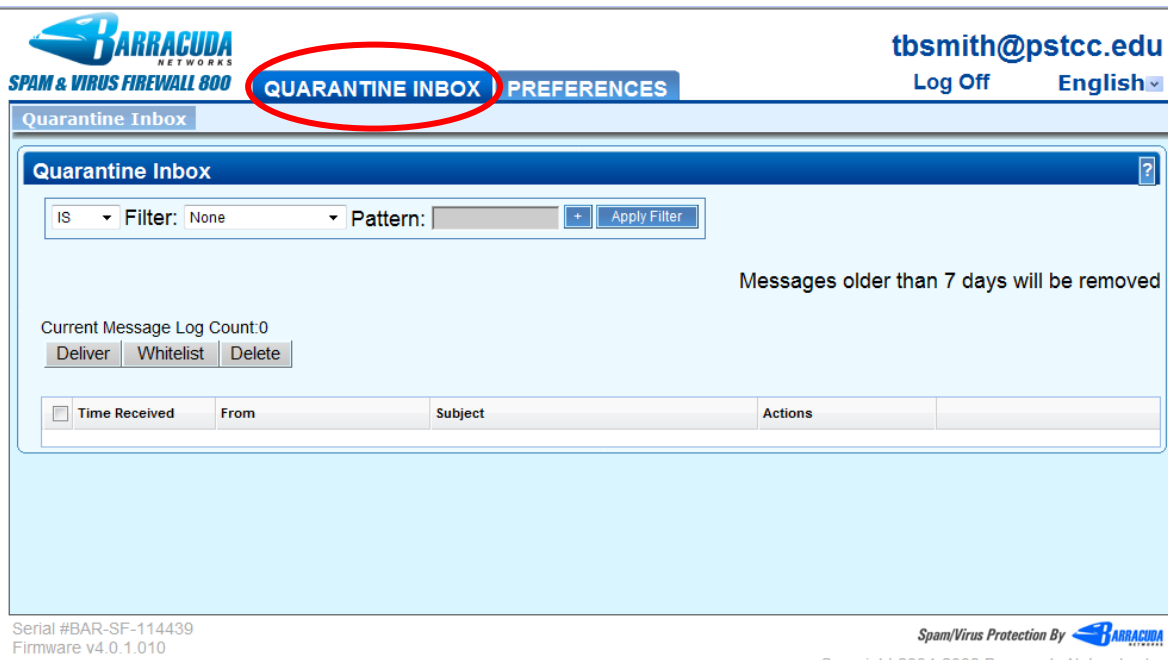
Barracuda Spam Firewall

Introduction:

The Barracuda SPAM appliance is now in place. With a little attention you will be able to curb the growing number of SPAM (unsolicited E-mail) messages that you receive each day. Though note that the prevention of ALL SPAM is virtually impossible. Mail that is considered SPAM by the Barracuda Firewall will “quarantine” the item in your personal SPAM folder. This means the message will not be delivered to your mail Inbox.

When you receive your first SPAM the system will send you a message containing a username/password (This is your AD account or otherwise the login you use to login to a campus PC.), and a link to a folder that allows you to access the suspect messages. As you receive mail suspected as SPAM, you will receive a daily message from the Barracuda Spam Firewall Service.

Here is an example of what you will see:



At this point, you will need to take action on the suspect mail. You will need to determine if each item is SPAM or legitimate mail. (You can read each message by clicking on the subject.)

Choices:

If the message is actually SPAM, then **delete** the message.

If the message is legitimate, then click on either 1) **Deliver** or 2) **Whitelist**

- ◆ **Deliver** means to allow the message to be sent to your mail Inbox for this one instance only.
- ◆ **Whitelist** means that the message will be sent to your Inbox and any future mail from the same address will also be allowed to pass through the filter. Please refer to Image 2 for Whitelist instructions.

We suggest you review the list, mark any messages as needed for **Deliver** and/or **Whitelist**, then simply

Select All and Delete or Classify as Spam

- ◆ **Delete** means it will only delete the current message
- ◆ **Classify as Spam** means it will delete it and block any incoming messages from this address

Alternatively, you may choose to deal with each message as you review the list.

If you review the list and see immediately that there are several items that need to be Delivered, Whitelist, Deleted or Classified as Spam, simply place a check beside each item and click on the appropriate option (Deliver or Whitelist or Delete or Classify as Spam).

Helpful Hints:

- ◆ If you do not receive mail suspected as SPAM, you will not receive the message from Barracuda Firewall.
- ◆ As you Release items, they will automatically be forwarded to your Inbox.
- ◆ The Whitelist\Blacklist tab under Preferences enables you to manage a list of specific addresses, domain names and usernames that will be accepted (as long as they comply with College policies) or blocked. It is also possible to enter addresses or domains. At the top on the right hand side, click on the Preferences tab, this will open a window that will allow you to enter a valid mail address (username@address.com) or domain name (everything after and including the @ sign) and click the allow or block button. Please see additional information attached.
- ◆ Mail that you delete will remain in the deleted items folder for 24 hours. At that time they will be permanently deleted. While in this folder, you can choose to release any item.
- ◆ Items not reviewed (deleted or released) will remain in your folder for 14 days then permanently deleted.
- ◆ Barracuda can be accessed via Outlook Client or Outlook Web Access (OWA).

Final Note:

As you create your Whitelist and Blacklist blocked messages to be marked as SPAM, less time will be required for reviewing the folder.

Advanced information on Whitelist\Blacklist:

Following is a detailed explanation of bulleted item above.

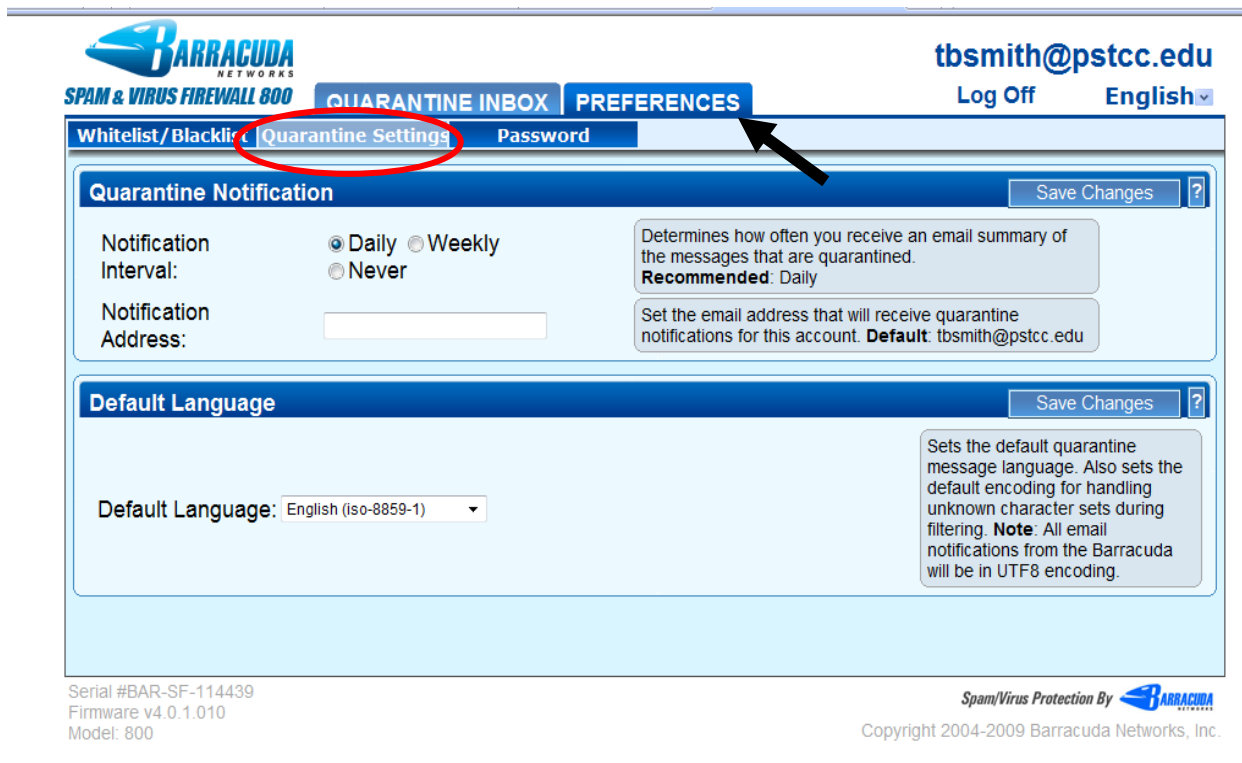
The **Whitelist\Blacklist** tab under the **Preferences** tab enables you to manage a list of specific addresses, domain names and usernames that will be accepted (as long as content complies with Barracuda RBLs and policies).

Your **Whitelist** is Allowed domains and e-mail addresses. Your **Blacklist** is Blocked domains and e-mail addresses. You can enter\view your domains and addresses manually from this or automatically from the Quarantine Inbox.

The screenshot shows the web interface of a Barracuda Spam & Virus Firewall 800. At the top left is the Barracuda Networks logo. At the top right, the user is logged in as **tbsmith@pstcc.edu** with options for **Log Off** and **English**. The main navigation bar includes **QUARANTINE INBOX** and **PREFERENCES**. Under **PREFERENCES**, the **Whitelist/Blacklist** sub-tab is selected and circled in red. Other sub-tabs are **Quarantine Settings** and **Password**. A green banner indicates **Configuration updated**. Below this are two sections: **Allowed Email Addresses and Domains (Whitelist)** and **Blocked Email Addresses and Domains (Blacklist)**. Each section has an **Email Address** input field, a **Bulk Edit** button, and an **Add** button. Explanatory text for each section states that email from these addresses will not be analyzed for spam (whitelist) or will always be blocked (blacklist). At the bottom left, system information is provided: **Serial #BAR-SF-114439**, **Firmware v4.0.1.010**, and **Model: 800**. At the bottom right, it says **Spam/Virus Protection By BARRACUDA** and **Copyright 2004-2009 Barracuda Networks, Inc.**

Quarantine Settings:

On the **Quarantine** tab under the **Preferences** tab you may make changes to disable Barracuda on your account and to set your Notification Interval.



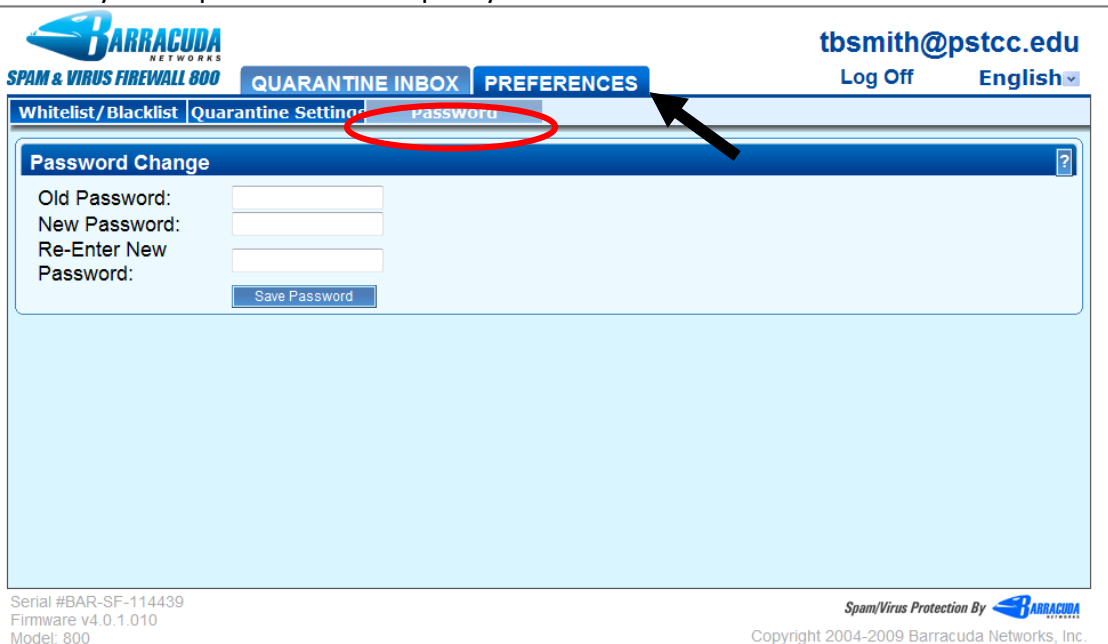
The screenshot shows the Barracuda Networks web interface. At the top, the user is logged in as **tbsmith@pstcc.edu**. The navigation menu includes **QUARANTINE INBOX** and **PREFERENCES**. Under **PREFERENCES**, the **Quarantine Settings** tab is highlighted with a red circle. An arrow points to the **PREFERENCES** tab. The main content area is divided into two sections:

- Quarantine Notification:** Includes radio buttons for **Notification Interval** (Daily, Weekly, Never) and a text field for **Notification Address**. A **Save Changes** button is present.
- Default Language:** Includes a dropdown menu for **Default Language** (set to English (iso-8859-1)) and a **Save Changes** button.

At the bottom, the serial number is **Serial #BAR-SF-114439**, the firmware is **Firmware v4.0.1.010**, and the model is **Model: 800**. The footer includes **Spam/Virus Protection By BARRACUDA** and **Copyright 2004-2009 Barracuda Networks, Inc.**

Password Change:

Initially your password is your AD account (The username\password used to login to campus PCs.). You can make changes to that on the **Password** tab under the **Preferences** tab. It is recommended though that you leave this as you AD password for simplicity.



The screenshot shows the Barracuda Networks web interface. At the top, the user is logged in as **tbsmith@pstcc.edu**. The navigation menu includes **QUARANTINE INBOX** and **PREFERENCES**. Under **PREFERENCES**, the **Password** tab is highlighted with a red circle. An arrow points to the **PREFERENCES** tab. The main content area is a **Password Change** section with the following fields:

- Old Password:** Input field
- New Password:** Input field
- Re-Enter New Password:** Input field
- Save Password:** Button

At the bottom, the serial number is **Serial #BAR-SF-114439**, the firmware is **Firmware v4.0.1.010**, and the model is **Model: 800**. The footer includes **Spam/Virus Protection By BARRACUDA** and **Copyright 2004-2009 Barracuda Networks, Inc.**