Barracuda Spam & Virus Firewall - *Quick Start Guide*

The Barracuda Spam & Virus Firewall is a spam and virus filtering appliance that filters email in front of your email server. It is physically installed on your network and assigned an IP address as a node on your internal network. It is common for the Barracuda Spam & Virus Firewall to be installed in the DMZ area of your network or behind a traditional firewall. The Barracuda Spam & Virus Firewall will filter out spam and viruses in a comprehensive fashion from your email before it is delivered to your email server.

1 Getting Started

This guide provides you with setup instructions for the Barracuda Spam & Virus Firewall. We recommend reading these instructions fully before starting the setup. To begin setting up your Barracuda Spam & Virus Firewall, you will need the following:

- Barracuda Spam & Virus Firewall, AC Power Cord (included)
- Mounting Rails (model 600/800/900 only)
- VGA Monitor (recommended)
- PS2 Keyboard (recommended)

2 Physical Installation

To install the Barracuda Spam & Virus Firewall:

1. Fasten the Barracuda Spam & Virus Firewall to a 19-inch rack or place it in a stable location.
2. Connect an Ethernet Cable from your network switch to the Ethernet port on the back of the Barracuda Spam & Virus Firewall.
3. Connect a Standard VGA Monitor, PS2 Keyboard, and AC power cord to the Barracuda. *Note*: Immediately after connecting an AC Power Cord to the Barracuda, it may power ON for a few seconds and then power OFF. This is because the Barracuda is designed to automatically return to a powered ON state in the event of a power outage.
4. Press the POWER button on the front panel to turn the Barracuda on.

3 Configure IP Address and Network Settings

If you have a monitor connected, the Barracuda Spam & Virus Firewall will display the Boot Menu initially, and the Administrative Console login prompt once fully booted. To begin the configuration:

1. Login to the Administrative Console using the admin login:
   - **Login**: `admin`
   - **Password**: `admin`

```
barracuda login: admin
password:
```

2. Configure the **IP Address, Subnet Mask, Default Gateway, Primary DNS Server** and **Secondary DNS Server** as appropriate for your network.
3. Save your changes.

If you do not have a monitor and keyboard and want to set the IP using the RESET button on the front panel, press and hold the RESET button per the following table:

IP address	Press and hold RESET for…
192.168.200.200	5 seconds
192.168.1.200	8 seconds
10.1.1.200	12 seconds

4 Opening Firewall Ports

If your Barracuda Spam & Virus Firewall is located behind a corporate firewall, open the following ports on your firewall to ensure proper operation:

Port	Direction	TCP	UDP	Usage
25	In/Out	Yes	No	Email and email bounces
53	Out	Yes	Yes	Domain Name Service (DNS)
80	Out	Yes	No	Virus, firmware and spam rule updates
123	Out	No	Yes	Network Time Protocol (NTP)

5 Barracuda Spam & Virus Firewall Configuration

Use a computer with a Web browser that is connected to the same network as the Barracuda and follow these steps:

1. In our Web browser's address bar, enter http:// followed by the Barracuda's IP address, followed by the default Web Interface HTTP Port (:8000). For example, if you configured the Barracuda with an IP address of 192.168.200.200, you would type: http://192.168.200.200:8000
2. Log in to the Barracuda Spam & Virus Firewall Web interface as the administrator: **Username:** admin **Password:** admin
3. Go to the **Basic→ IP Configuration** page and perform the following:
   - Verify that the **IP Address**, **Subnet Mask**, and **Default Gateway** are correct.
   - Enter the **Server Name/IP** of your destination email server where you want the Barracuda to deliver mail. For example, type: mail.<yourdomainname>.com
   - Verify that the **Primary** and **Secondary DNS Server** are correct.
   - Enter **Default Hostname** and **Default Domain**. This is the name that will be associated with bounced messages. For example, enter *barracuda* as the Default Hostname and <yourdomain.com> as the Default Domain.
   - Under **Allowed Email Recipient Domain(s)**, enter each domain for which the Barracuda will receive email. Click **Add** after each domain entry. *Note: The Barracuda will reject all incoming email addressed to domains not specified here.*

4. Click any one of the **Save Changes** buttons to save all of the information.
5. **MODEL 100 ONLY:** Go to the **Users** page and perform ***at least one*** of the following:
   - Enter the email address(es) on which the Barracuda is to perform spam and virus scanning under **User Configuration**, one entry per line.
   - To have email addresses automatically added to the Barracuda as mail arrives, make sure the **Enable User Addition** option is turned on.

   ***Note**: If no users are specified, AND the **Enable User Addition** option is set to "no", then no scanning of ANY incoming email will be performed.*
6. Save your changes.

6 Update the Firmware

Go to **Advanced→Firmware Update**. If there is a new **Latest General Release** available, perform the following steps to update the system firmware:

1. Click on the **Download Now** button located next to the firmware version that you wish to install. To view download progress, click on the **Refresh** button. When the download is complete, the **Refresh** button will be replaced by an **Apply Now** button.
3. Click on the **Apply Now** button to install the firmware. This will take a few minutes to complete. To avoid damaging the Barracuda, do not manually power OFF the system during an update or download.
4. After the firmware has been applied, the Barracuda Firewall will automatically reboot, and displays the login page when the system has come back up.
5. Log back into the Web interface again and read the Release Notes to learn about enhancements and new features. It is also good practice to verify settings you may have already entered, as new features may have been included with the firmware update.

7 Change the Administrator Password

To avoid unauthorized use, we recommend you change the default administrator password to a more secure password. You can only change the administrator password for the Web interface. You cannot change the password for the Administrative Console, but this is only accessible via the keyboard which you can disconnect at any time.

1. Go to **Basic→Administration** and enter your old and new passwords.
2. Click on **Save Password**.

8 Product Activation

Verify that the Energize Updates feature is activated on your Barracuda by going to the **Basic→Status** page. Under Subscription Status, make sure the Energize Updates subscription is Current. If the Energize Updates is Not Activated, click the corresponding activation link to go to the Barracuda Networks Product Activation page and complete activation of your subscriptions.

9 Route Email to the Barracuda Spam & Virus Firewall

To take advantage of the spam and virus filtering features of the Barracuda Spam & Virus Firewall, you must route all incoming email to the Barracuda. There are two common options for routing email to the Barracuda Spam & Virus Firewall:

- **Port Forwarding**. Change the port forwarding settings on your corporate firewall to route incoming email to your Barracuda Spam & Virus Firewall. To do this, modify your corporate firewall port settings as required. For instructions, see your firewall documentation or administrator.
- **MX Records**. Create a DNS entry for your Barracuda Spam & Virus Firewall and change your DNS MX record to route incoming email to the Barracuda. Typically, this is done at your DNS server or through your DNS service.

  Example: *DNS Entry for Barracuda Spam & Virus Firewall*

  ```
  barracuda.barracudanetworks.com  IN A  66.233.233.88
  ```

  Example: *Modified MX Record*

  ```
  IN MX 10       barracuda.barracudanetworks.com
  ```

Although DNS programs and services vary, your new DNS and MX entries should resemble the examples above. The above example shows a priority of 10, for illustration only. *Note: Some DNS servers cache information for up to 7 days, so it may take time for your email to be routed to the new MX record.*

10 Important Items

- Do not try to route outgoing email through the Barracuda Spam & Virus Firewall unless you have configured Relay operation or are using the Barracuda Spam & Virus Firewall in Outbound Mode.
- We recommend turning off all spam controls on your email server in order to eliminate potential conflicts.

11 Tuning your Spam Controls

Initially your Barracuda Spam & Virus Firewall is configured to Tag most spam. The subject line of the spam messages will be prepended with the word "[BULK]". This allows user configuration of email client programs to put the messages into a separate folder. You can adjust the aggressiveness of the spam scoring algorithm at any time. These changes can easily be made on the **Basic→ Spam Scoring** page. We recommend using an initial configuration that does only tagging. After you have some familiarity and see how email is being tagged you can adjust the configuration to suit your needs.

For additional documentation including an Administrator's Guide, visit **http://www.barracuda.com/documentation**.

Contact and Copyright Information
Barracuda Networks, Inc. 3175 S. Winchester Blvd, Campbell, CA 95008 USA • phone: 408.342.5400 • fax: 408.342.1061 • www.barracuda.com