

The Barracuda Spam & Virus Firewall Vx Virtual Appliance includes the same powerful technology and simple Web based user interface found on the Barracuda Spam & Virus Firewall hardware appliance. It is designed for easy deployment on VMware infrastructure and can be combined with other Barracuda Networks hardware appliances. The virtual appliance is a good option for standardizing hardware platforms or for deploying a Barracuda Spam & Virus Firewall solution in an existing virtual environment. As the organization grows, it can be scaled for performance and capacity and also provides for quick backup and disaster recovery. The Barracuda Spam & Virus Firewall Vx supports version 4.1 and higher of the Barracuda Spam & Virus Firewall firmware.

Before downloading and installing your Barracuda Spam & Virus Firewall Vx, make sure you have the following in place:

- A configured server running the VMware ESXi server version 3.5, Update 2, or higher on which you will install the Barracuda Spam & Virus Firewall Vx.
- The **VMware vSphere** client installed on your local machine.
- 6 GB of free space on your VM client (local) machine if you are using the ZIP download method of getting the virtual machine image as described below.

Installing the Virtual Appliance Image

From the [Virtual Machines Downloads Web page](#), there are two methods for obtaining the virtual appliance image for the Barracuda Spam & Virus Firewall Vx:

- **Method 1: Download the Open Virtual Machine Format (OVF) Template from Barracuda Central** by copying and pasting the URL from the Virtual Machines Downloads page into your VM client. This method is more convenient, but requires the bandwidth to download the entire virtual appliance image once for each installation of the virtual appliance. If you are only going to download one virtual appliance / product, this method is suggested.
- **Method 2: Download the ZIP archive of the OVF Template** directly from the Virtual Machines Downloads page (Figure 2). If you are going to deploy multiple Barracuda Network virtual appliances, this method will save time and bandwidth by only downloading once. You can simply re-use the same ZIP file for each virtual appliance installation.

Installation Method 1: Download the OVF Template from Barracuda Central

1. Log in to your VM vSphere client.
2. From your VM vSphere client interface, select the **File > Deploy OVF Template** option to create the virtual appliance.
3. Select **Deploy by URL** and copy and paste the URL from the Virtual Machines Downloads page as shown in Figure 1.

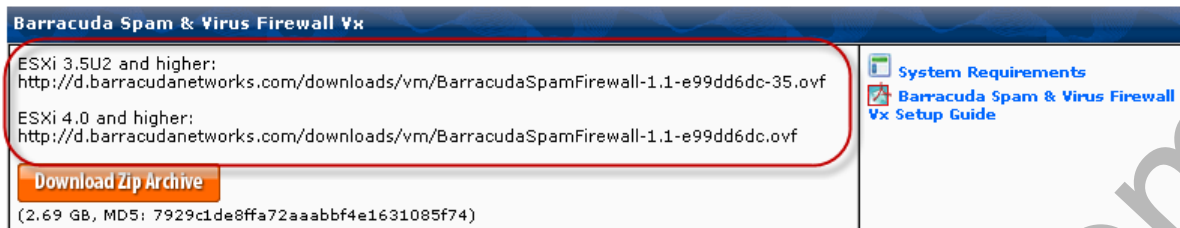


Figure 1. Virtual Machines Downloads page for getting the virtual appliance image

4. Read and accept the license agreement.
5. Give the virtual appliance a name, such as, for example, "Library Spam & Virus Firewall".
6. In your VM vSphere client, choose a data store to use for your Barracuda Spam & Virus Firewall Vx virtual appliance.
7. Review the options you've selected before clicking **Finish** to start the deployment task. The task could take awhile as the product image downloads.
8. When you see the **Deployment Complete** window, close it, and you should see your new virtual appliance listed by the name you gave it in the left sidebar of the VM vSphere client.
9. After installation, if desired, you can **Edit Settings** by right clicking on the virtual appliance to configure memory, number of virtual processors and other settings before starting it.

Installation Method 2: Download the ZIP archive of the OVF Template

1. From the Virtual Machines Downloads page click on the link for the zip file for the product image. Downloading the image could take a few minutes.



Figure 2. Click on the ZIP archive to download the product image

2. Unzip the ZIP archive, which contains the following files, on your system:
 - The OVF template, which is an .ovf file. THIS is the file you will import to your VM client in step 5 below.
 - The product image, which is a .vmdk file
 - A checksum file (.mf)
 - A README file and additional notes as applicable
 - End-User License Agreement
3. Log in to your VM vSphere client.
4. From your VM vSphere client interface, select the **File > Deploy OVF Template** option to create the virtual appliance.
5. Select **Deploy from file** and click the **Browse** button to locate the OVF template (the .ovf file) you unpacked from the ZIP archive on your local file system or network.

6. Read and accept the license agreement.
7. Give your virtual appliance a name that will easily identify it in your VM vSphere Client, for example: "Library Spam & Virus Firewall Firewall".
8. In your VM vSphere client, choose a data store to use for your Barracuda Spam & Virus Firewall Vx virtual appliance.
9. Review the options you've selected before clicking **Finish** to start the deployment task.
10. After installation, if desired, you can **Edit Settings** by right clicking your virtual appliance in the left pane of the VM vSphere client to configure memory, number of virtual processors and other settings before starting it.

Configuring the Virtual Appliance Template

1. Once the virtual appliance is downloaded to your VM Client, you can click on it to select it, then click the **Run** icon or menu option to run the virtual appliance.
2. Once your virtual appliance is running, click the **Console** tab to use the console configuration utility. You'll see the system starting up, which could take a minute or two. Log in with the username **admin** and a password of **admin**.

NOTE: Your mouse will be 'captured' by the VM client; press <ctrl><alt> to see your mouse again on the screen.

3. When you see the *System Configuration* screen, using your keyboard arrow keys, arrow down to 'TCP/IP Configuration' and set the IP address, netmask, gateway, and DNS addresses for this appliance. Arrow down to **Save** and hit Enter to commit the change.
4. Arrow down to 'Licensing', hit Enter and key in your license using the token from the Customer Services email message you received from Barracuda Networks. Enter the default domain you want to use for this virtual appliance.
5. Arrow down to **Save** and hit Enter to commit the change.

Opening Firewall Ports

If your Barracuda Spam & Virus Firewall Vx 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)

Logging into the Barracuda Spam & Virus Firewall Vx Web interface

Once the virtual appliance has been configured, visit the virtual appliance Web interface and use it like any other Barracuda Networks product. You can access the appliance by entering the following URL in your browser, replacing **<MyVxIPAddress>** with the IP address you entered in the console configuration utility above:

`http://<MyVxIPAddress>:8000`

Verify the configuration by following these steps:

1. Log into the Barracuda Spam & Virus Firewall Vx Web interface as the administrator. Use **Username:** admin **Password:** admin
2. Go to the Basic→IP Configuration page and perform the following:
 1. Verify that the **IP Address**, **Subnet Mask**, and **Default Gateway** are correct.
 2. Enter the **Server Name/IP** of your destination email server where you want the Barracuda to deliver mail. For example, type: **mail.<yourdomainname>.com**
 3. Verify that the **Primary** and **Secondary DNS Server** are correct.
 4. 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.
 5. 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.*
3. Click any one of the **Save Changes** buttons to save all of the information.

Update the Firmware

Click on the Advanced→Firmware Update page. 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.
2. Click on the **Apply Now** button to install the firmware. This will take a few minutes to complete.
3. After the firmware has been applied, the Barracuda Spam & Virus Firewall Vx will automatically reboot, displaying the login page when the system has come back up.
4. 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.

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. Go to Basic→Administration and enter your old and new passwords, then click on **Save Password**.

Route Email to the Barracuda Spam & Virus Firewall

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

- **Port Forwarding.** Change the port forwarding settings on your corporate firewall to route incoming email to your Barracuda Spam & Virus Firewall Vx. 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 Vx 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.

Outgoing Email

Do not try to route outgoing email through the Barracuda Spam & Virus Firewall Vx unless you have configured Outbound Relay operation on the ADVANCED → Outbound page.

Tuning your Spam Controls

Initially your Barracuda Spam & Virus Firewall Vx 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.

Best Practices for Configuring your VMware vSphere Client

Barracuda Networks recommends the following for best configuration of your VM client running the Barracuda Spam & Virus Firewall Vx:

1. Allocate 1 GB of RAM for the virtual appliance per CPU allocated and 40 GB of available hard disk space.
2. You will need only a single virtual NIC on your virtual appliance. Most likely you will want to use the 'bridged' networking setup on VMware.

Note: VMware tools are not needed for Barracuda Networks virtual appliances (they mostly have to do with graphical interface characteristics for virtual desktop OSs).

Online help is available by clicking the Help icon on any page of the product Web interface. The Barracuda Spam & Virus Firewall Vx Administrator's guide covers concepts and advanced topics for administering the product and can be found on the Barracuda Networks Web site at <http://www.barracuda.com/documentation>

Backing Up Your Barracuda Virtual Appliance System State

Virtual machine environments generally provide a "snapshot" capability, which captures the state of a system as it's running. Once a snapshot is created, you can perform additional operations on the system and "revert" to the snapshot in the case of disaster recovery (or for any other reason).

Because this feature is so powerful, Barracuda Networks **very strongly** recommends performing a snapshot at certain points in time:

1. Before upgrading the Barracuda Virtual Appliance firmware.
2. Before making major changes to your configuration (this makes snapshotting a convenient "undo" mechanism).
3. After completing and confirming a large set of changes, such as initial configuration.
4. As a periodic backup mechanism.

Barracuda Networks also strongly recommends that you review your virtual environment documentation regarding snapshotting capabilities and be familiar with their features and limitations.