

The Barracuda SSL VPN Vx Virtual Appliance includes the same powerful technology and simple Web based user interface found on the Barracuda SSL VPN 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 SSL VPN solution in an existing virtual environment. As the organization grows, it can be scaled for performance and capacity and also provides quick backup and disaster recovery.

Before downloading and installing your Barracuda SSL VPN Vx, make sure you have the following in place:

- A configured server running the VMware ESXi server version 3.5 or higher.
- 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 SSL VPN Vx:

- **Method 1: Download the 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 client.
2. From your VM 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 for your ESXi version 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 SSL VPN".
6. In your VM client, choose a data store to use for your Barracuda SSL VPN 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 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 file to download the product image

2. Unzip the ZIP archive, which contains the following three 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)
3. Log in to your VM client.
4. From your VM 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 Client, for example: "Library SSL VPN Firewall".
8. In your VM client, choose a data store to use for your Barracuda SSL VPN 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 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. 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 SSL VPN 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 alerts and one-time passwords
53	Out	Yes	Yes	Domain Name Service (DNS)
80	Out	Yes	No	Virus, firmware and updates
123	Out	No	Yes	Network Time Protocol (NTP)
443	In/Out	Yes	No	HTTPS/SSL port for SSL VPN access
8000	In/Out	Yes	No	Appliance administrator interface port (HTTP)
8443	In/Out	Yes	No	Appliance administrator interface port (HTTPS)

Note: The Appliance Administrator interface ports on 8000/8443 should only be opened if you intend to manage the appliance from the Internet.

Logging into the Barracuda SSL VPN 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 SSL VPN Vx Web interface as the administrator. Use **Username:** admin **Password:** admin
2. Go to the Basic→IP Configuration page and perform the following:
 - a. Verify that the **IP Address**, **Subnet Mask**, and **Default Gateway** are correct.
 - b. Verify that the **Primary** and **Secondary DNS Server** are correct.
 - c. Verify that the Proxy Server Configuration settings are correct, if you are using a proxy server on your network.
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 SSL VPN 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 Incoming SSL Connections to the Barracuda SSL VPN

To take advantage of the features of the Barracuda SSL VPN Vx, you must route HTTPS incoming connections on port 443 to the virtual appliance. This is typically achieved by configuring your corporate firewall to port forward SSL connections directly to the Barracuda SSL VPN Vx.

Note: The Appliance Administrator Web interface ports on 8000/8443 will also need similar port forward configurations if you intend to manage the appliance from outside the corporate network.

Verify Incoming Connections to the Barracuda SSL VPN

Once you have configured your corporate firewall to route SSL through to the Barracuda SSL VPN, you should be able to accept incoming SSL connections.

1. To test the connection, use a Web browser from the Internet (not inside the LAN) to establish an SSL connection to the external IP address of your corporate firewall. For example, if your firewall's external IP address is 192.168.1.1, connect your browser to: `https://192.168.1.1`.
2. You should be prompted to accept an un-trusted SSL certificate, which will cause a warning message to appear in your browser. Accept the warning and proceed to load the page.
3. You should be prompted with the login page for the SSL VPN User Interface. Log in with the credentials for the VPN administrator:

Login: **ssladmin**
Password: **ssladmin**

4. You should now be successfully logged in as the VPN administrator, and taken directly to the SSL VPN Management Interface. From here you can set up accounts and other resources for users of the Barracuda SSL VPN.

Best Practices for Configuring your VMware vSphere Client

Barracuda Networks recommends the following for best configuration of your VM client running the Barracuda SSL VPN Vx:

1. Allocate 1 GB of RAM for the virtual appliance per CPU allocated.
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.
3. If you're going to use the Barracuda SSL VPN Vx *Network Connector*, you should enable *Promiscuous Mode* in your **VMware vSphere** client:
 - In the client, click on the Configuration tab.
 - Click on the *Networking* link on the left navigation bar.
 - Click on the *Properties* link to the right of the Virtual Switch pane.
 - In the Virtual Switch properties window, click on VM Network on left navigation bar (your network name may differ).
 - Click the **Edit** button at bottom, select the Security tab, click the box for Promiscuous Mode, select **Accept** from the drop-down and click the **Okay** button.

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

Post Setup Configuration Items

Your Barracuda SSL VPN should now be configured at a basic level to accept incoming connections from the Internet. Online help is available by clicking the Help icon on any page of the product Web interface. The **Barracuda SSL VPN 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>

Refer to the Administrator's Guide as necessary for more details regarding the following additional steps:

- Register a hostname with your DNS server for the Barracuda SSL VPN, e.g. sslvpn.company.com
- Install an SSL certificate on the Barracuda SSL VPN for this hostname to ensure that your users are able to determine that they are connecting to a genuine Barracuda SSL VPN that is registered to your organization.
- Integrate the Barracuda SSL VPN with your existing user database. To cleanly integrate with your environment, the Barracuda can read in user accounts and authenticate against a number of different databases, including Microsoft Active Directory.
- Grant access to resources to your SSL VPN users. See the documentation for more information on the usage of the policy based access control framework.
- If your network uses a DMZ, you may wish to configure the Barracuda SSL VPN in this topology for greater security.

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.