

How to Deploy Barracuda SSL VPN Vx Images

<https://campus.barracuda.com/doc/39813153/>

Barracuda Networks offers the following types of images for the Barracuda SSL VPN Vx deployment. Follow the instructions for your hypervisor to deploy the Barracuda SSL VPN Vx appliance.

Image Type	Supported Hypervisors
OVF	<ul style="list-style-type: none">• esxi4• VMware ESX and ESXi (vSphere Hypervisor) version 5.x and 6.x• Sun/Oracle VirtualBox and VirtualBox OSE 3.2
VMX	<ul style="list-style-type: none">• VMware Server 2.0+• VMware Fusion 3.0+, Player 3.0+, and Workstation 6.0+
XVA	<ul style="list-style-type: none">• Citrix XenServer 5.5+
VHD	<ul style="list-style-type: none">• Microsoft Hyper-V 8, 8.1, 2012, 2012 R2, and 10

You can download these images from the [Barracuda Virtual Appliance Download page](#). After the download is complete, extract the files from the ZIP folder.

If you are deploying the Barracuda SSL VPN Vx on a VMware hypervisor, complete [How to Configure VMware ESXi for the Barracuda SSL VPN](#) after deploying the VM.

Deploy OVF images

VMware ESX and ESXi (vSphere Hypervisor) 4.x

Use the OVF file ending in **-4x.ovf** for this hypervisor.

1. [Download](#) and expand the Barracuda SSL VPN Vx ZIP folder.
2. From the **File** menu in the vSphere client, select **Deploy OVF Template**.
3. Select **Import from file** and navigate to the extracted folder and locate the Barracuda SSL VPN OVF file. Click **Next**.
4. Enter a name for the virtual appliance.
5. Set the network to point to the target network for this virtual appliance.
6. Follow the recommendations in [Allocating Cores, RAM, and Hard Disk Space for Your Barracuda SSL VPN Vx](#).
7. After your appliance has finished importing, right-click it, select **Open Console**, and click the green arrow to power on the virtual appliance.
8. Follow the [Barracuda SSL VPN Vx Quick Start Guide](#) instructions to set up your virtual appliance.

VMware ESX and ESXi (vSphere Hypervisor) 5.x and 6.x

Use the OVF file ending in **-5x.ovf** or **-6x.ovf** for this hypervisor.

1. [Download](#) and expand the Barracuda SSL VPN Vx ZIP folder.
2. From the **File** menu in the vSphere Client, select **Deploy OVF Template**.
The vSphere Client launches the **Deploy OVF Template** wizard.
3. Click **Browse**, navigate to the extracted folder, and locate the Barracuda Web Filter Vx OVF file. Click **Next**.
4. Verify that you are installing the correct Barracuda virtual appliance. Click **Next**.
5. Enter a name for the virtual appliance. Click **Next**.
6. Select the destination storage for the virtual machine. Click **Next**.
7. Select a disk format. To ensure maximum stability when deploying your Barracuda Vx appliance, specify the disk format as **Thick Provision Eager Zeroed**. Click **Next**.
8. Map the network to the target network for this virtual appliance. Click **Next**.
9. Review the deployment options. Click **Finish** to deploy the virtual appliance.
10. Follow the recommendations in [Allocating Cores, RAM, and Hard Disk Space for Your Barracuda SSL VPN Vx](#).
11. Locate the appliance within the appropriate virtual machine and resource pool. Select it and power it on by clicking the green arrow.
12. Click the **Console** tab. You can monitor the appliance as it is prepared for use.
13. Follow the [Barracuda SSL VPN Vx Quick Start Guide](#) instructions to set up your virtual appliance.

Sun/Oracle VirtualBox and VirtualBox OSE 3.2

Use the OVF file ending in **-4x.ovf** for this hypervisor.

1. [Download](#) and expand the Barracuda SSL VPN Vx ZIP folder.
2. From the **File** menu in the VirtualBox client, select **Import Appliance**.
3. Navigate to the extracted folder and locate the Barracuda SSL VPN OVF file.
4. Select the file and click **Next**.
5. On the **Import Settings** screen, follow the recommendations in [Allocating Cores, RAM, and Hard Disk Space for Your Barracuda SSL VPN Vx](#). Click **Finish**.
6. Start the appliance.
7. Follow the [Barracuda SSL VPN Vx Quick Start Guide](#) instructions to set up your virtual appliance.

Deploy VMX images

VMware Server 2.x

Use the **.vmx** and **.vmdk** files for this hypervisor.

1. [Download](#) and expand the Barracuda SSL VPN Vx ZIP folder.
2. Move the files ending in **.vmx** and **.vmdk** into a folder in your datastore (which you can locate from the **Datastores** list on your server's summary page).
3. From the VMware Infrastructure Web Access client's **Virtual Machine** menu, select **Add Virtual Machine to Inventory**.
4. Navigate to the folder in your datastore used in step 2 and select the file ending in **.vmx**. Click **OK**.
5. Navigate to the folder used in step 2 and select the **BarracudaSSLVPN.vmx** file from the list under **Contents**. Click **OK**.
6. Follow the recommendations in [Allocating Cores, RAM, and Hard Disk Space for Your Barracuda SSL VPN Vx](#).
7. Start the appliance.
8. Follow the [Barracuda SSL VPN Vx Quick Start Guide](#) instructions to set up your virtual appliance.

VMware Player 3.x, Fusion 3.x, and Workstation 6.x

VMware Player cannot edit the network or vswitch settings. This can cause problems when testing the Network Connector.

Use the **.vmx** file for these hypervisors.

1. [Download](#) and expand the Barracuda SSL VPN Vx ZIP folder.
2. From the **File** menu, select **Open a Virtual Machine**.
3. Select the **BarracudaSSLVPN.vmx** file.
4. Use the default settings, and click **Finish**.
5. Follow the recommendations in [Allocating Cores, RAM, and Hard Disk Space for Your Barracuda SSL VPN Vx](#).
6. Start the appliance.
7. Follow the [Barracuda SSL VPN Vx Quick Start Guide](#) instructions to set up your virtual appliance.

Deploy XVA images

Citrix XEN Server 5.5+

Use the **.xva** file for this hypervisor. For XEN Server, you first import the virtual appliance template and then create a new virtual appliance based on that template.

Step 1. Import the virtual appliance template:

1. [Download](#) and expand the Barracuda SSL VPN Vx ZIP folder.

2. From the **File** menu in the XenCenter client, select **Import**.
3. Click **Browse**, navigate to the extracted folder, and select the file ending in **.xva**. Click **Next**.
4. Select a server for the template. Click **Next**.
5. Select a storage repository for the template. Click **Import**.
6. Select a virtual network interface for the template. Click **Next**.
7. Review the template settings. Click **Finish** to import the template.

Step 2. Create a new virtual appliance:

1. Right-click the virtual appliance template and select **New VM wizard**.
2. Select the virtual appliance template. Click **Next**.
3. Enter a name for the virtual appliance. Click **Next**.
4. For the DVD drive, select **<empty>**. Click **Next**.
5. Select a home server. Click **Next**.
6. Specify the number of virtual CPUs and memory for the virtual appliance. Follow the recommendations in [Allocating Cores, RAM, and Hard Disk Space for Your Barracuda SSL VPN Vx](#). Click **Next**.
7. Select a virtual disk. Click **Next**.
8. Select a virtual network interface. Click **Next**.
9. Review the virtual appliance settings. Click **Create Now**.
10. When the virtual appliance is ready, right-click it and then click **Start**.
11. Follow the [Barracuda SSL VPN Vx Quick Start Guide](#) instructions to set up your virtual appliance.

Deploy VHD images

Microsoft Hyper-V 8, 8.1, 2012, 2012 R2, and 10

Use the **.vhd** file for this hypervisor.

1. [Download](#) and expand the Barracuda SSL VPN Vx ZIP folder.
2. Launch the *WinServerSetup.bat* file located in the extracted folder. This batch file corrects a compatibility issue and takes less than a minute to run.
3. Navigate to the extracted folder and verify that the **HyperV** folder contains the following sub-folders:
 - **Snapshots**
 - **Virtual Hard Disks**
 - **Virtual Machines**
4. In Hyper-V Manager, right-click the VM host and select **Import Virtual Machine**.
5. On the **Before You Begin** page of the **Import Virtual Machine** wizard, click **Next**.
6. On the **Locate Folder** page:
 1. Click **Browse**, navigate to the extracted folder, and select the **HyperV** folder. Click **Select Folder**.
 2. Click **Next**.
7. On the **Select Virtual Machine** page, click **Next**.

8. On the **Choose Import Type** page, select **Copy the virtual machine (created a new unique ID)**. Click **Next**.
9. On the **Choose Destination: Choose Folders for Virtual Machine Files** page, click **Browse** to search for the location where you want to store the VM files. Click **Next**.
10. On the **Choose Storage Folders: Choose Folders to Store Virtual Hard Disks** page, click **Browse** to search for the location where you want to store the virtual hard disks for the VM. Click **Next**.
11. For Microsoft Windows 10, you can modify the RAM and Hard Disk space allocations after completing step 12.
On the **Configure Memory** page, enter a size for the **Startup RAM** that meets the requirements at [Allocating Cores, RAM, and Hard Disk Space for Your Barracuda SSL VPN Vx](#). Keep the default settings for the other fields. Click **Next**.
12. On the **Connect Network** page, select the network interface that you want to use for management access of the VM. Click **Next**.
13. On the **Summary** page, verify that all the settings are correct. Click **Finish**.
14. For Microsoft Windows 10, go to the **Actions** pane and click on **Settings** under **Barracuda SSL VPN**. Under Hardware, ensure that there is enough memory and hard disk space as specified in [Allocating Cores, RAM, and Hard Disk Space for Your Barracuda SSL VPN Vx](#).
15. Start your virtual appliance.
16. Follow the [Barracuda SSL VPN Vx Quick Start Guide](#) instructions to set up your virtual appliance.

To take advantage of Microsoft's VHDX support on Hyper-V 2012, 2012 R2 and 10, follow the instructions in [How to Convert and Replace a Barracuda Virtual Appliance VHD File with a VHDX Format File](#).

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.