

How to Deploy a CloudGen Firewall Vx OVA on VMware Hypervisors

<https://campus.barracuda.com/doc/79463320/>

If you are deploying the Barracuda CloudGen Firewall Vx in a high performance environment or require support for VLANs, do not deploy using the OVA packages. Instead, create a custom configuration using Barracuda F-Series Install. For more information, see [How to Deploy a CloudGen Firewall Vx using F-Series Install on a VMware Hypervisor](#).

To ease deployment, the Barracuda CloudGen Firewall Vx units are available as prebuilt OVA images that can be imported into your VMware hypervisor. You do not need to create or configure a virtual machine (VM). Before deploying the CloudGen Firewall Vx unit, verify that the host system meets the minimum storage requirements and review the resource recommendations for the production system. You can deploy the firewall using either the VMware vSphere Client or the VMware OVF Tool (ovftool).

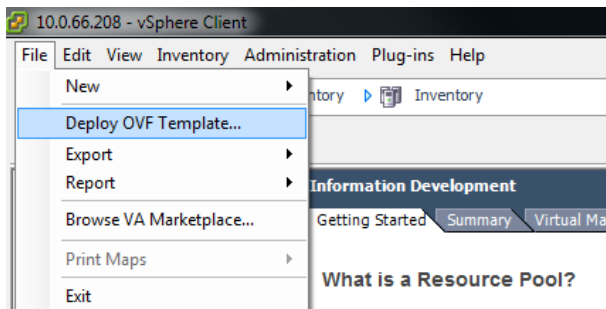
Before You Begin

- For information regarding the sizing of your CPU, disk, and RAM, see [Virtual Systems \(Vx\)](#).
- Before you start the Barracuda CloudGen Firewall Vx for the first time, assign a manual MAC address to the first virtual network interface. This lets you move the VM later without invalidating your license. For more information, see [Best Practice - Performance Tuning on VMware Hypervisors](#).
- Download the VMware OVA image from the [Barracuda Download Portal](#).

Use the VMware vSphere Client

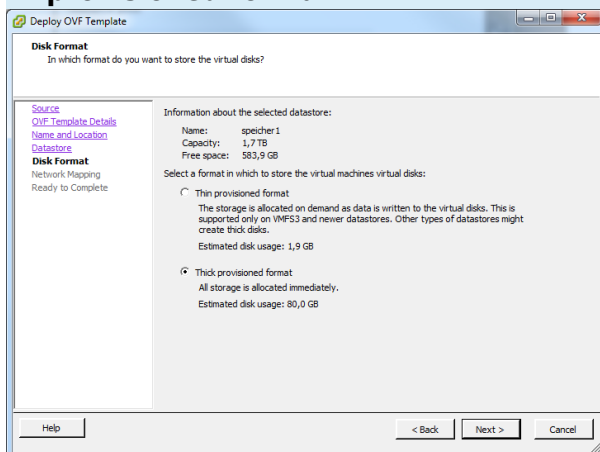
Step 1. Download and Import the OVA Image

1. Download the OVA image for your CloudGen Firewall or Firewall Control Center from your [Barracuda Networks Account](#).
2. Connect to your VMware hypervisor using the vSphere client.
3. Click **File > Deploy OVF Template**.

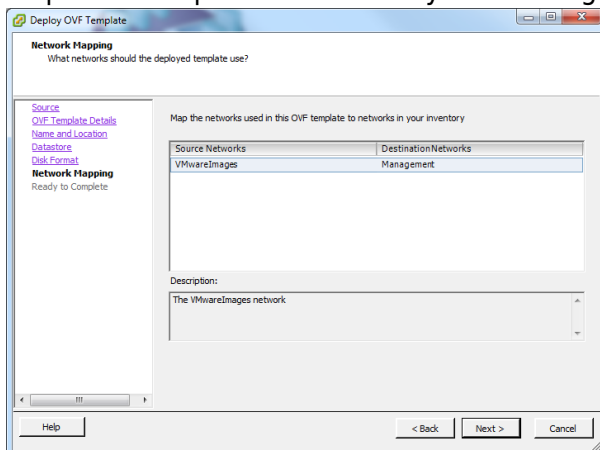


4. In the deployment wizard, click **Browse** and select the OVA image. Click **Next** to proceed.
5. Enter a name for the virtual machine to be created. Click **Next** to proceed.
6. Select the datastore that the CloudGen Firewall Vx unit should be installed on.

When you import an OVA file with VMware 4.1 and later, you are offered the **Thin provisioned format** setting that lets you change the VM size. If you choose to reduce the VM size, do not choose a value below 50 GB for VFxxx or a value below 100 GB for VC400, VC610, or VC820. Barracuda Networks recommends that you select **Thick provisioned format**.



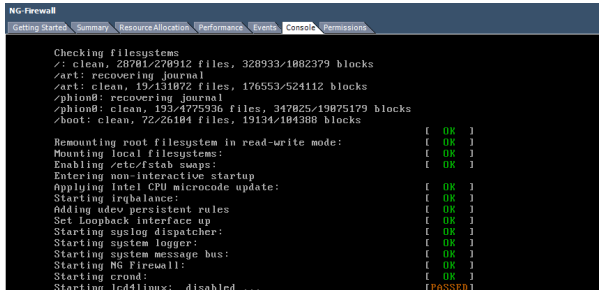
7. Map to the required network in your existing inventory and then click **Next** to proceed.



8. After the deployment wizard summarizes all your settings, click **Finish** to start the deployment process. After successful deployment, the Barracuda CloudGen Firewall Vx unit is displayed in your VMware hypervisor inventory list.
9. Select the CloudGen Firewall Vx unit from the list on the left and edit settings such as **Disk Provisioning** with appropriate values.

Step 2. Set the Management IP Address

1. Start the VM and click the **Console** tab of the virtual machine. The Barracuda CloudGen Firewall Vx unit boots.

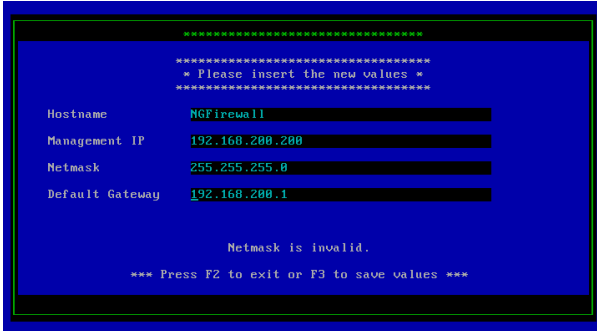


```

NG-Firewall
Getting Started Summary Resource Allocation Performance Events Console Permissions
Checking filesystems
/: clean, 28701/270912 files, 328933/1082379 blocks
/art: recovering journal
/phiomd: recovering journal
/phiomd: clean, 193/4775936 files, 347025/19075179 blocks
/boot: clean, 72/26104 files, 19134/104308 blocks

Remounting root filesystem in read-write mode: [ OK ]
Mounting local filesystems: [ OK ]
Enabling rc/rcsda sweeps: [ OK ]
Entering non-interactive startup [ OK ]
Applying Intel CPU microcode update: [ OK ]
Starting irqbalance: [ OK ]
Adding udev persistent rules [ OK ]
Set Loopback interface up [ OK ]
Starting syslog dispatcher: [ OK ]
Starting system logger: [ OK ]
Starting system message bus: [ OK ]
Starting NG Firewall: [ OK ]
Starting cron: [ OK ]
Starting lcd4linux: disabled ... [POSSE]
  
```

For a basic network configuration, the CloudGen Firewall unit launches the **Active Recovery Technology** menu.



```

*****
*****
* Please insert the new values *
*****
*****
Hostname      NGFirewall
Management IP 192.168.200.200
Netmask       255.255.255.0
Default Gateway 192.168.200.1

Netmask is invalid.

*** Press F2 to exit or F3 to save values ***
  
```

2. Select **Basic Configuration**, enter the following network settings, and then press **F3** to save your changes:
 - **Hostname** – The desired hostname for your firewall.
 - **Management IP** – The IP address that your firewall should be reachable through.
 - **Netmask** – The subnet mask in dotted quad notation. For example, 255 . 255 . 255 . 0.
 - **Default Gateway** – The IP address of the next hop device that serves as an access point to another network.
3. When the window opens to announce that your configuration changes were saved, press any key to continue.
4. Select **Reboot** to restart the Barracuda CloudGen Firewall with the new network configuration.

Use the VMware OVF Tool

1. Download the VMware OVF Tool from vmware.com. Use the following command:
`ovftool -datastore= datastore name ovaimage vi://server-ip`
 where:
 - `datastore` – The name for the data store.
 - `ovaimage` – The path and name of the OVA file.
 - `server-ip` – The IP address for the virtual appliance.
2. Configure the resources pool and the network mapping within the VMware virtual machine settings.
3. Using Barracuda Firewall Admin, connect to the virtual appliance for configuration.

Use the latest version of Barracuda Firewall Admin. If you configure the Barracuda CloudGen Firewall with a version of Barracuda Firewall Admin that is older than the firewall version, you might lose configuration data.

Next Step

After you deploy the Barracuda CloudGen Firewall Vx unit, continue with [Getting Started](#) and optionally [Best Practice - Performance Tuning on VMware Hypervisors](#).

Figures

1. Deploy_Template.png
2. Disk_Format.png
3. Network_Mapping.png
4. virtual-boot.png
5. ART_Console.png

© Barracuda Networks Inc., 2019 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.