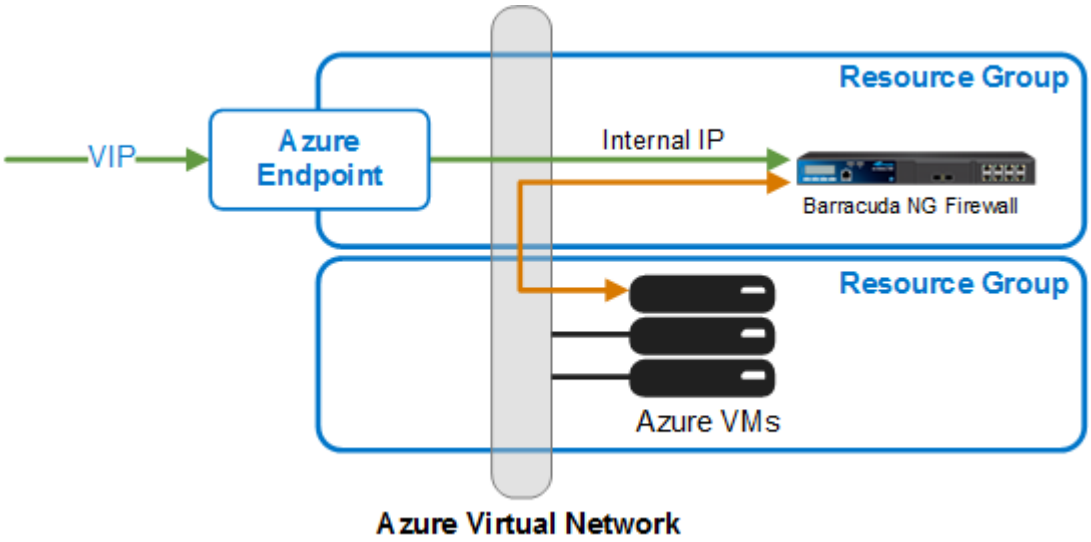
How to Deploy the Barracuda NG Firewall in Microsoft Azure

https://campus.barracuda.com/doc/43847088/

Only Barracuda NG Firewall BYOL images are available when deploying via Azure Portal. For more information, see Public Cloud Hosting.

The Barracuda NG Firewall Azure can be deployed as a virtual machine in the Microsoft Azure cloud. You can use up-to-date Application Control 2.0, user awareness, integrated malware protection, and VPN services to securely handle and manage all traffic in your virtual network.

Microsoft Azure charges apply. For more information, see the Microsoft Azure Pricing Calculator.



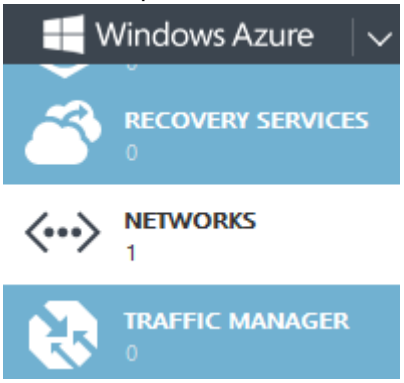
In this article

Before you Begin

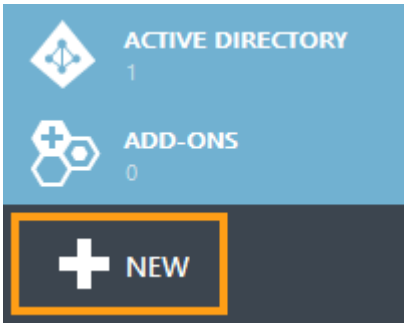
- Create a Microsoft Azure account.
- Get a Barracuda NG Azure license from the Barracuda Networks Evaluation page:
  1. From the **Select a Product** list, select **Barracuda NextGen Firewall** under the **Public Cloud Solutions** category.
  2. From the **Select Edition** list, select the Level that you want.
  3. Complete and submit the rest of the form. You will receive an email containing your serial number and license token.

Step 1. Create an Azure Virtual Network

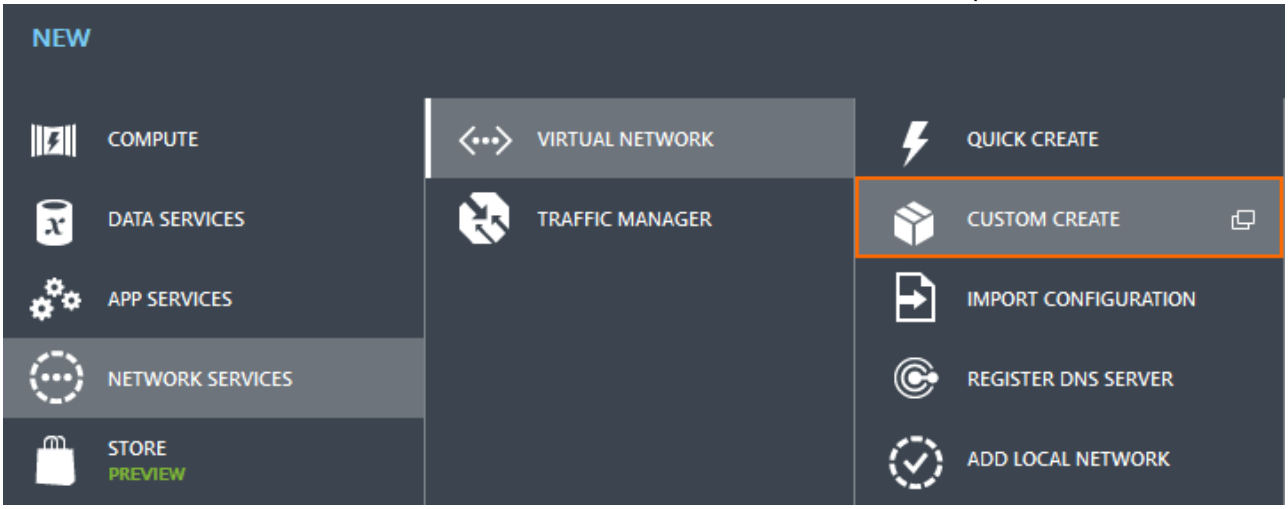
1. Log into your Microsoft Azure Management Portal (https://manage.windowsazure.com)
2. In the left pane, click **NETWORKS**.



3. In the bottom left corner, click **+ NEW**.

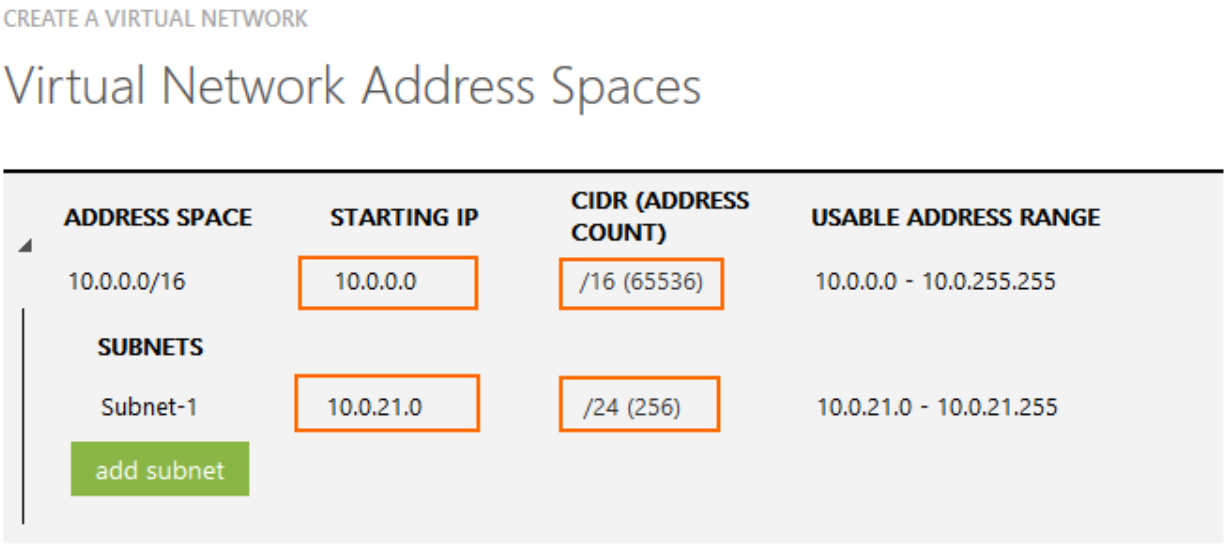


4. Click **CUSTOM CREATE**. The **CREATE A VIRTUAL NETWORK** window opens.



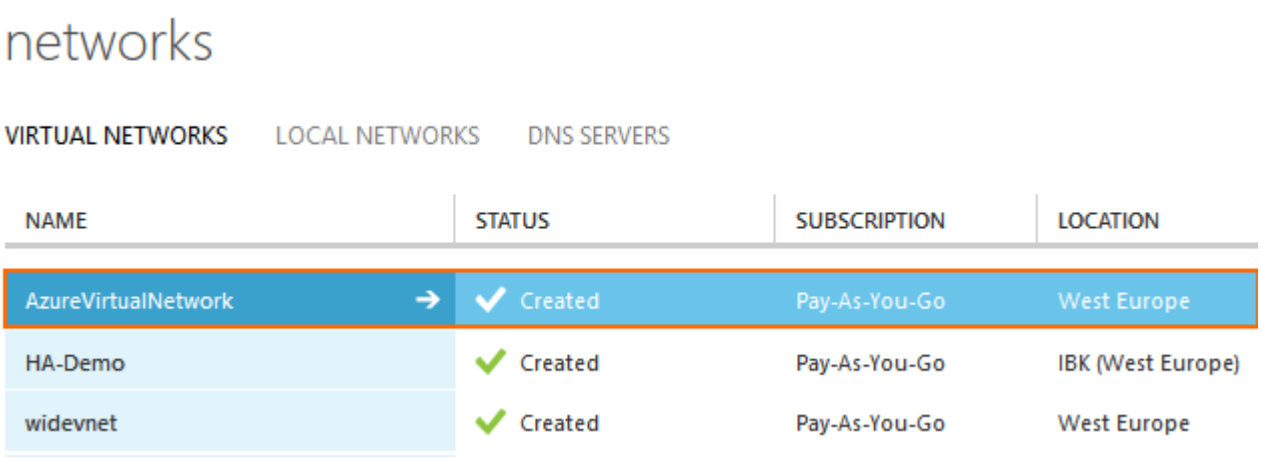
5. **Enter** a unique **NAME**. E.g., `AzureVirtualNet`
6. Select a **LOCATION**. The virtual network can only be used for Azure VMs in this geographic region. E.g., **West Europe**

7. Click **Next**.
8. (Optional) Select or enter your **DNS SERVERS**.
9. Click **Next**.
10. On the **Virtual Network Address Space** configure the **ADDRESS SPACE**:
    - **STARTING IP** – Enter the first IP address of the address space you want to use. E.g., `10.0.0.0`
    - **CIDR** – Select the subnet mask for the virtual network. The maximum number of VMs for a virtual network are listed in parentheses. E.g., **/16 (65536)**
11. Add a **SUBNET**
    - **STARTING IP** – Enter the fist IP address of the subnet. E..g, `10.0.21.0`
    - **CIDR** – Select the subnet mask for the subnet. E.g., **/24 (256)**



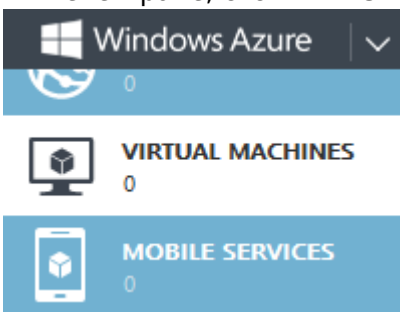
12. Click **FINISH**.

The virtual network is now listed in **VIRTUAL NETWORKS**.

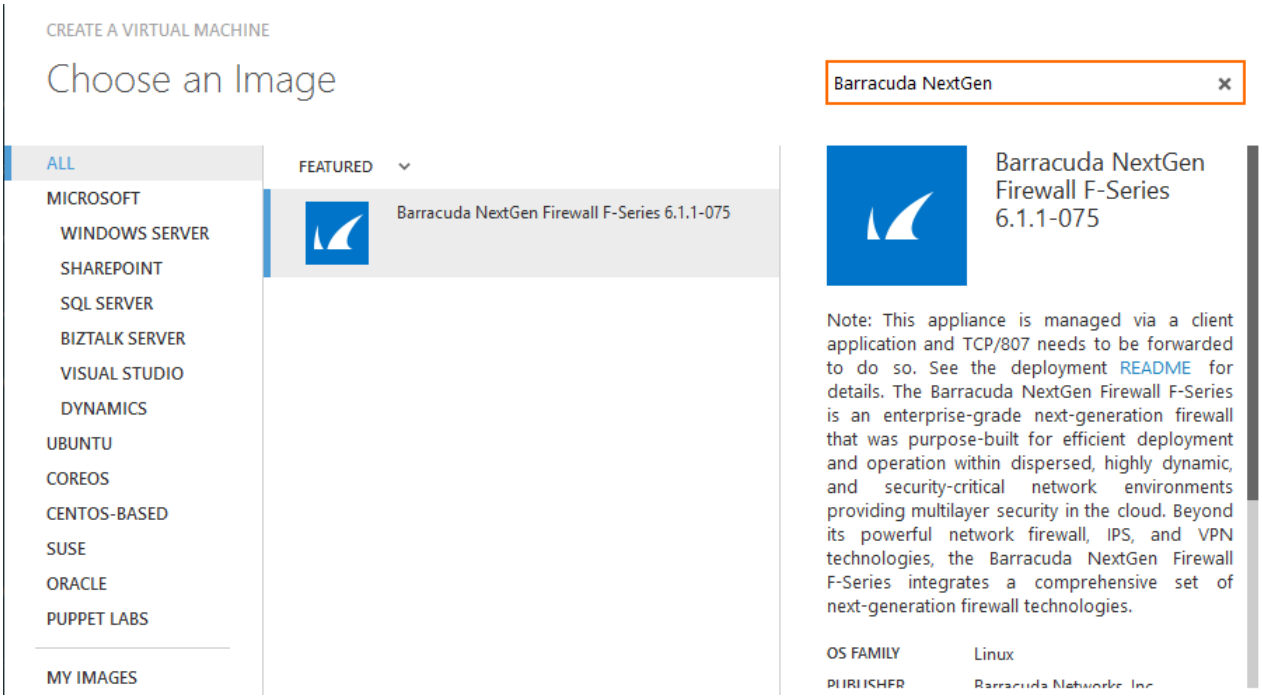


Step 2. Launch the Barracuda NG Virtual Machine Instance

1. Log into your Microsoft Azure Management Portal (https://manage.windowsazure.com).
2. In the left pane, click **VIRTUAL MACHINES**.

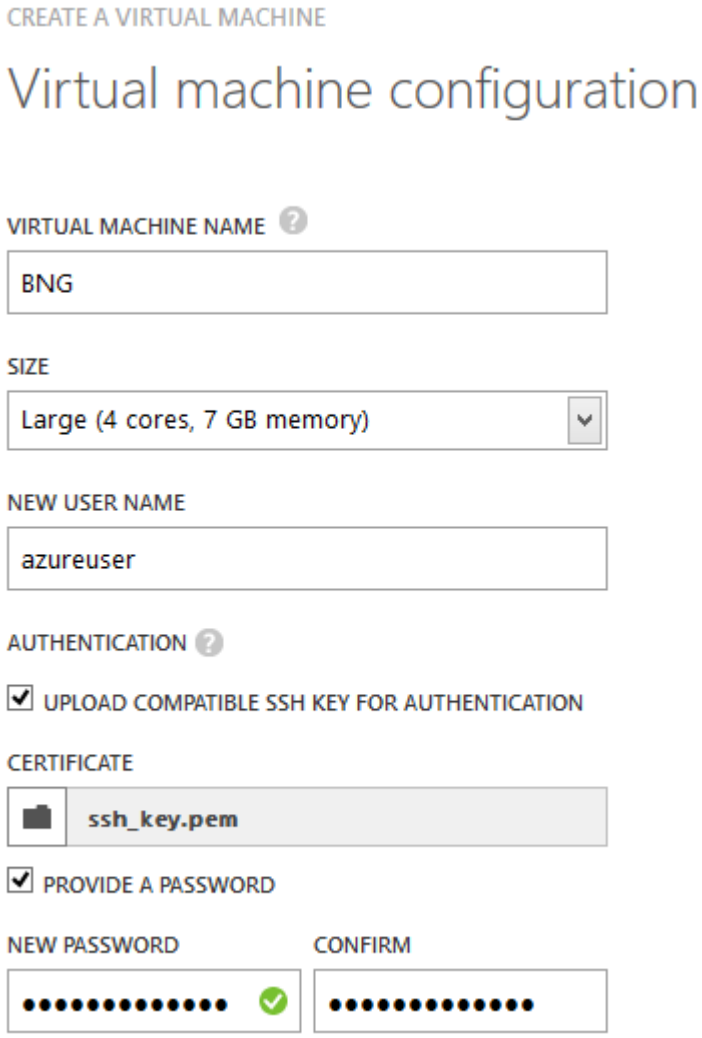


3. Click **NEW** in the bottom left-hand corner.
4. Click **FROM GALLERY**. The **CREATE A VIRTUAL MACHINE** windows opens.
5. In the search bar on the top left enter `Barracuda NG Firewall`. The **Barracuda NG Firewall 6.1** image is displayed in the **Featured** column.
6. From the **FEATURED** column in the middle pane, select **Barracuda NG Firewall 6.1**.

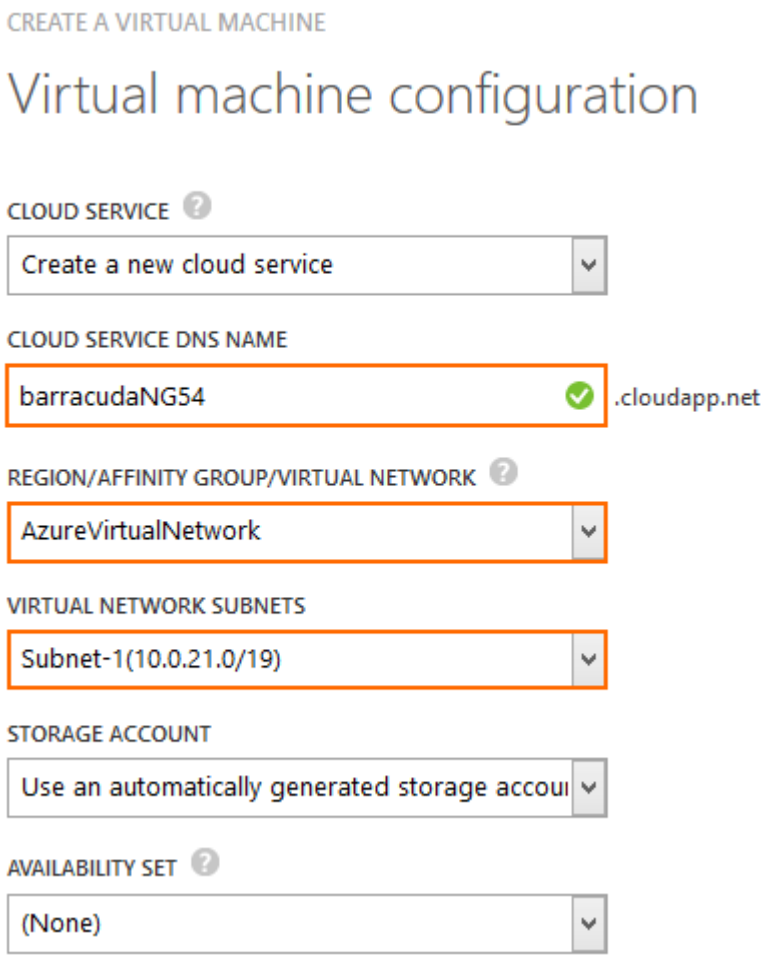


7. Click **NEXT**.
8. Enter the following settings in the **Virtual machine configuration**:
   - **VIRTUAL MACHINE NAME** – Enter the name for the virtual Barracuda NG Firewall (e.g., BNG). The name must be unique in the domain.
   - **SIZE** – Select an instance level that matches your Barracuda NG Firewall Azure license (e.g., Level 2 (1 CPU cores), Level 4 (2 CPU cores)).
   - **NEW USER NAME** – This entry is not used by the Barracuda NG Firewall. You may enter a random username.
   - **PASSWORD** – Select **PROVIDE A PASSWORD** and enter the root password for the Barracuda NG Firewall.

     After deploying your Barracuda NG Firewall the initial, three day, grace period starts. You must complete licensing during the initial grace period or the unit will switch into demo mode and the default root password (`ngf1r3wall`) is enabled.



9. Click **Next**.
10. Enter a **CLOUD SERVICE DNS NAME** The name must be unique for the used domain. (e.g., `barracudaNG60`).



11. Enable Barracuda NG Admin access to the new Barracuda NG Firewall instance by adding the following endpoints:

NAME	PROTOCOL	PUBLIC PORT	PRIVATE PORT
SSH	TCP	22	22
NG Admin TCP	TCP	807	807

12. Click **FINISH**.

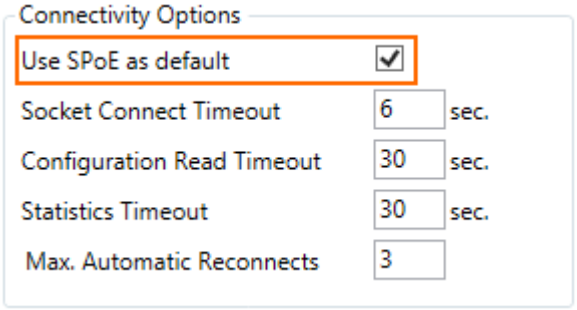
Step 3. Configure Barracuda NG Admin

You must use the latest version of **Barracuda NG Admin** to connect to your Barracuda NG Firewall Azure.

Enable support for Microsoft Azure in NG Admin.

1. Launch NG Admin.
2. In the upper left hand corner, click **Options** and select **Settings**.

3. In the **Client Settings** section, verify that the check box for **SPoE as default** is ticked.



Next Steps

- You can now connect to your Barracuda NG Firewall in the Microsoft Azure cloud.
- On the Barracuda NG Firewall, enter the license token and serial number that you received from Barracuda Networks.
- To use two Barracuda NG Firewalls in a high availability (HA) cluster, see How to Configure a High Availability Cluster in Azure.
  To use Public Instance Level IPs, Reserved IPs, or other advanced Azure networks setups, see Reserved, Static and Public IP Addresses in the Azure Cloud using ASM

To continue setting up your Barracuda NG Firewall, see Getting Started.

Figures

1. AzureDeploymentPreviewPortal.png
2. AzureNetwork01.png
3. AzureStorage02.png
4. AzureNetwork02.png
5. AzureNetwork03.png
6. AzureNetwork04.png
7. AzureNetwork05.png
8. AzureInstance01.png
9. AzureInstance02.png
10. AzureInstance03.png
11. AzureInstance04.png
12. SPoE02.png
13. SPOE.png