How to Deploy a CloudGen Firewall from the Microsoft Azure Marketplace

https://campus.barracuda.com/doc/95259238/

You can install the Barracuda CloudGen Firewall as a virtual machine in the Microsoft Azure public cloud. The Azure Solution Template deploys a single firewall into a dedicated subnet of a new or existing Virtual Network.Centrally managed firewalls get their configuration from the Control Center.

You can choose between the following images in the Azure Marketplace:

- **Bring Your Own License (BYOL)** – Uses licenses purchased directly from Barracuda Networks. Barracuda Networks offers a 30-day evaluation license.
- **Pay As You Go (PAYG)** – No dedicated licenses required. Licensing fees are included in the hourly price of the virtual machine. All charges are billed directly through your Microsoft Azure account.

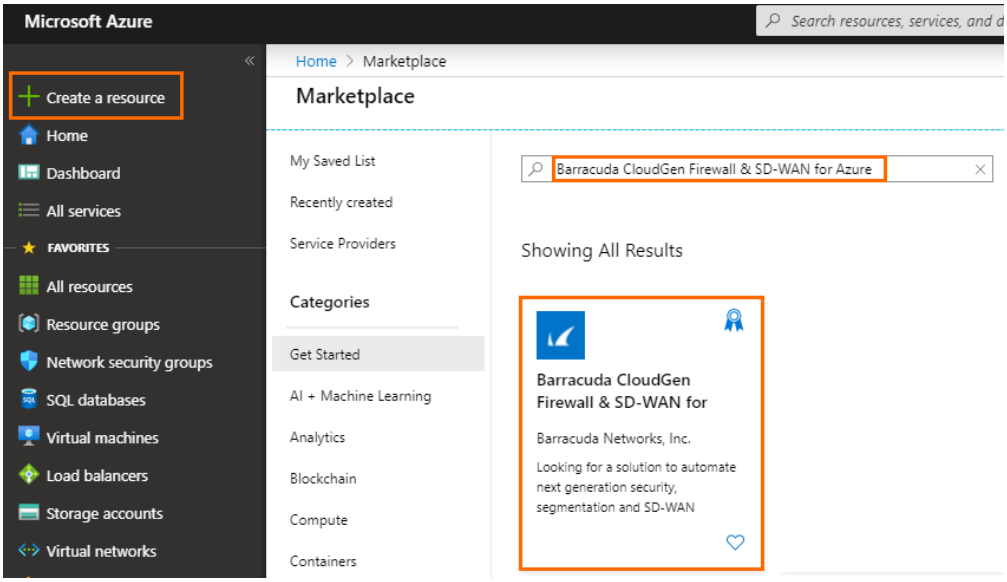
Depending on your deployment, you may want to use more than one resource group to be able to maintain the deployed VMs more easily.

Before You Begin

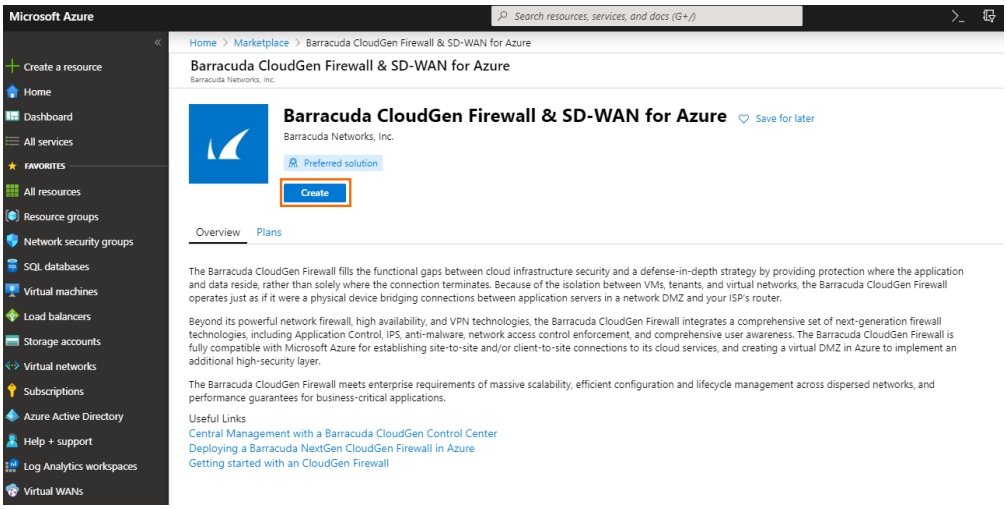
- Create a Microsoft Azure account.
- (BYOL images only) Purchase a Barracuda CloudGen Firewall or Control Center for Microsoft Azure license, or register to receive an evaluation license from the Barracuda Networks Evaluation page.

Step 1. Basics

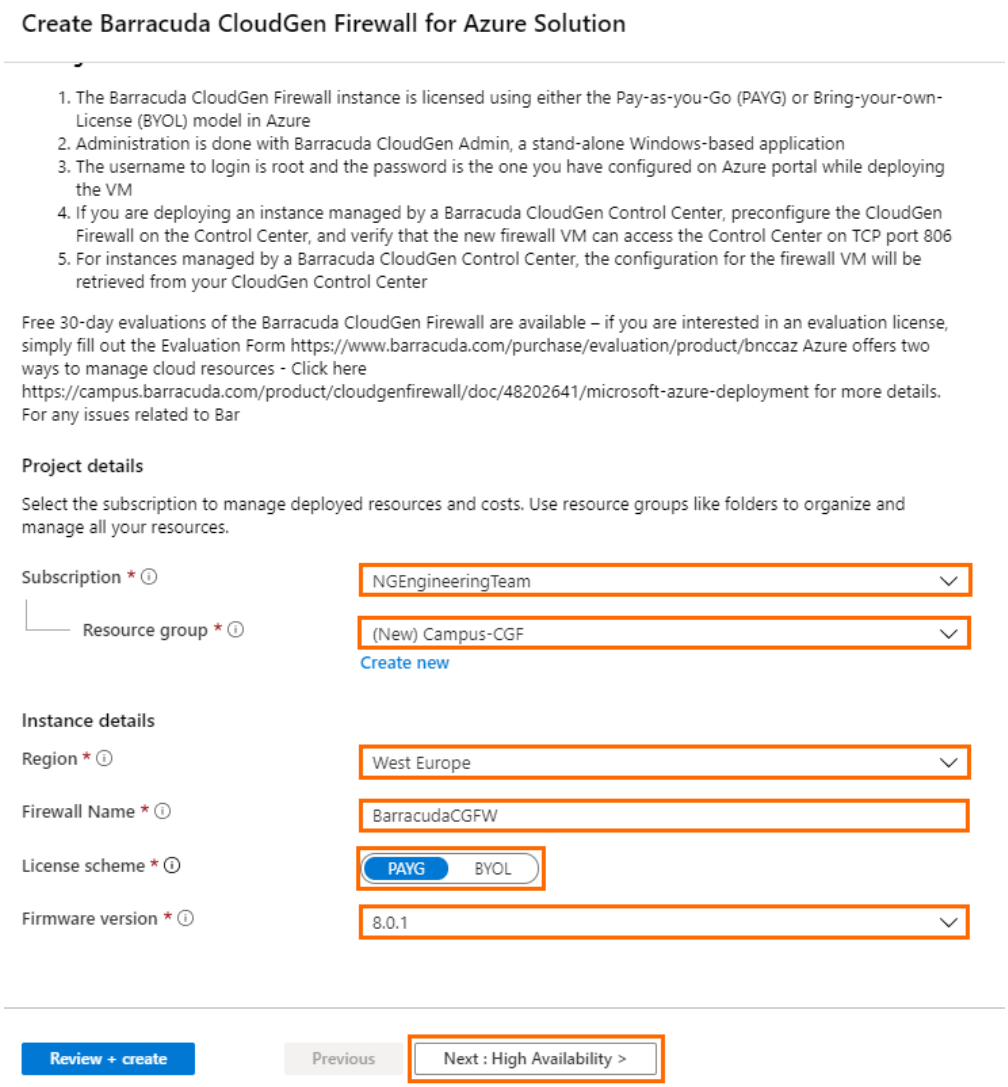
1. Go to the Azure portal: https://portal.azure.com
2. In the upper left-hand corner, click **+ Create a resource**.
3. Search the Marketplace for `Barracuda CloudGen Firewall & SD-WAN for Azure` and click **Barracuda CloudGen Firewall & SD-WAN for Azure**.



4. In the next window, click **Create**.



5. In the **Basics** blade, configure the following settings:
   - **Subscription** – Select your subscription.
   - **Resource Group** – Select an existing resource group to deploy to, or click **Create new** for a new resource group.
   - **Region** – Select the desired location the firewall will be deployed to.
   - **Firewall Name** – Enter the hostname for the CloudGen Firewall.
   - **License scheme** – Select either **PAYG** or **BYOL**.
   - **Firmware version** – Select one of the available firmware versions. Barracuda Networks recommends deploying the highest available version.

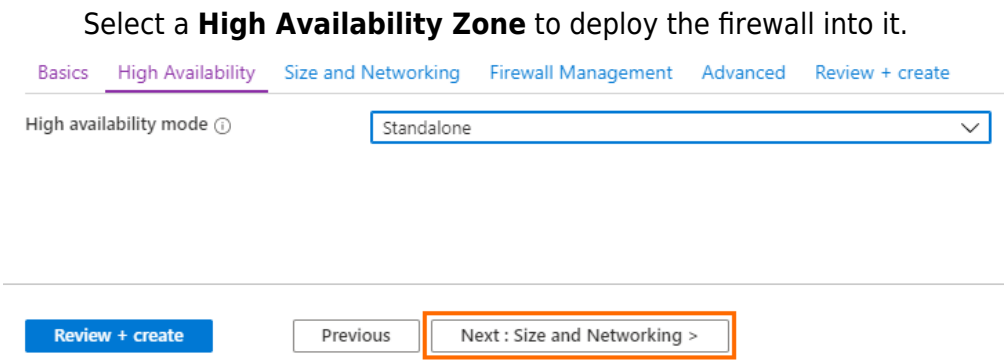


6. Click **Next : High Availability >**.

Step 2. High Availability

In this blade you can create either a high availability cluster or a single firewall.

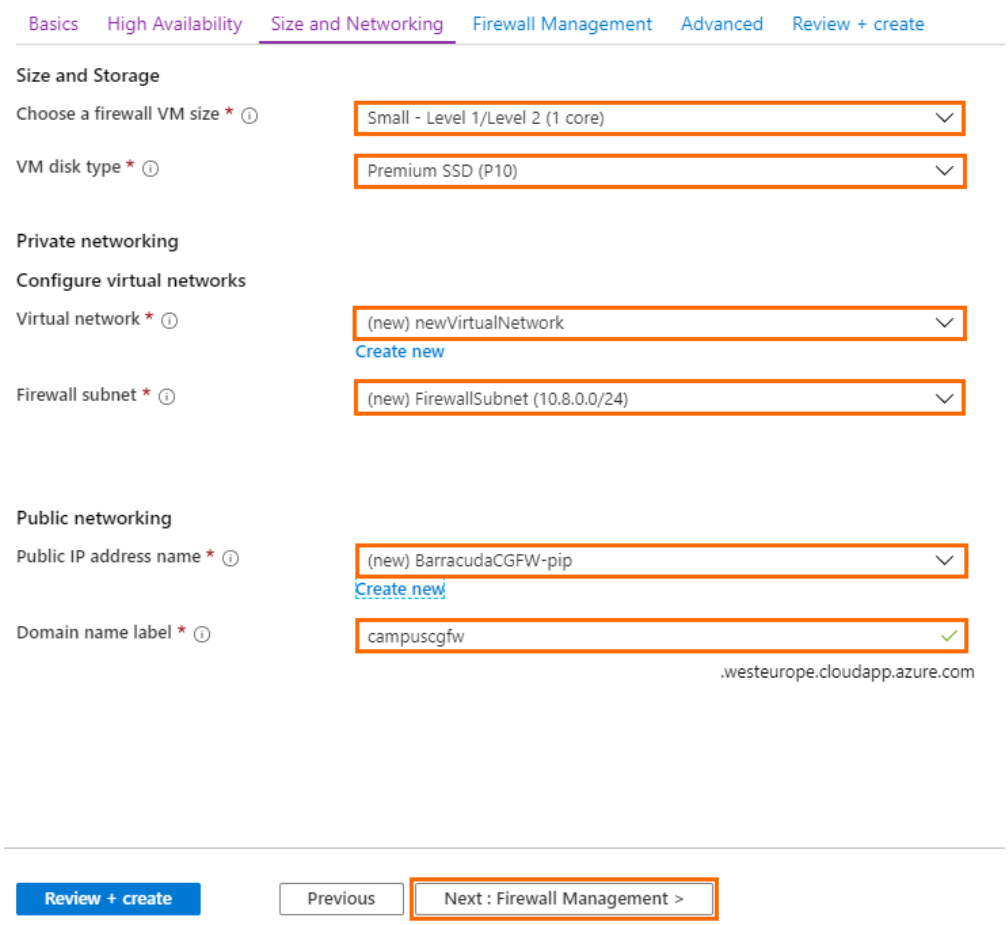
1. **High availability mode** – Select from the drop-down menu if you want to deploy a single firewall or a high availability cluster. The following options are available:
   - **Active/passive HA cluster** – Deploys a high availability (HA) cluster. For more information, see How to Deploy a High Availability Cluster with Cloud Integration from the Microsoft Azure Marketplace.
   - **Standalone** – Deploys a single firewall.
   - **Standalone in availability set** – Deploys a single firewall in an availability set. Enter an **Availability set name**. If this set does not exist, it will be created automatically.
   - **Standalone in availability zone** – Deploys a single firewall in an availability zone.



2. Click **Next : Size and Networking >**.

Step 3. Size and Networking

1. In the **Size and Networking** blade, configure the following settings:
   - **Choose a firewall VM size** – Select the size of the virtual machine
     To enable Azure Accelerated Networking either during this deployment or later through CLI, the size of your virtual machine must meet the requirements of Microsoft.
   - **VM disk type** – Select the disk type of your firewall virtual machine.
   - **Virtual network** – Select an existing **Virtual network** , or create a new one.
   - **Firewall subnet** – Select an existing subnet, or create a new one. This subnet will host your firewall. The firewall must be placed in a different subnet than the protected instances.
   - **Public IP address name** – Select an existing **Public IP address**, or create a new one. If you are using high availability, select a **Standard** SKU public IP.
     Note that regardless of the option selected, the Barracuda CloudGen Firewall is always deployed with a standard SKU public IP address for enhanced performance. For example, if you select a basic SKU IP address, the CloudGen Firewall will still be deployed with a standard SKU IP address.
   - **Domain name label** – Enter a domain name for your firewall.



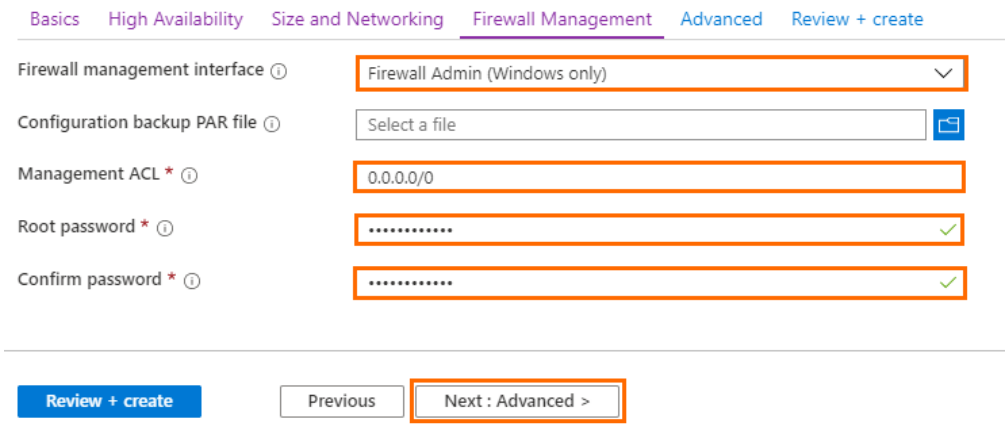
2. Click **Next : Firewall Management >**.

Step 4. Firewall Management

1. In the **Firewall Management** blade, configure the following settings.
   - **Firewall management interface** – Select the management interface type for your Barracuda CloudGen Firewall. You can choose between **Firewall Admin (Windows only)**, **Web Interface** and **Centrally managed via Control Center**. For more information on each topic, see Barracuda Firewall Admin, Web Interface, and Firewall Control Center. For a Control Center-managed firewall you need the configuration backup PAR file, the IP address of the Control Center, the Control Center Range ID, the Cluster name, and the PAR file retrieval key.

     The firewall management interface cannot be changed after deployment. If the web interface is enabled, central management with the Control Center is not possible.
   - **Configuration backup PAR file** – Select an unencrypted configuration backup to restore a firewall configuration. Make sure that static IP addresses, hostname and licenses of the configuration backup match the configuration of the virtual machine.
   - **Management ACL** – Introduces a Network Security Group that restricts access to management ports of the firewall. Enter `0.0.0.0/0` to allow access from any network

and to skip creating a Network Security Group.
- **Root password** – Enter the password for the **root** user of the firewall.
- **Confirm password** – Retype the password for the **root** user of the firewall.

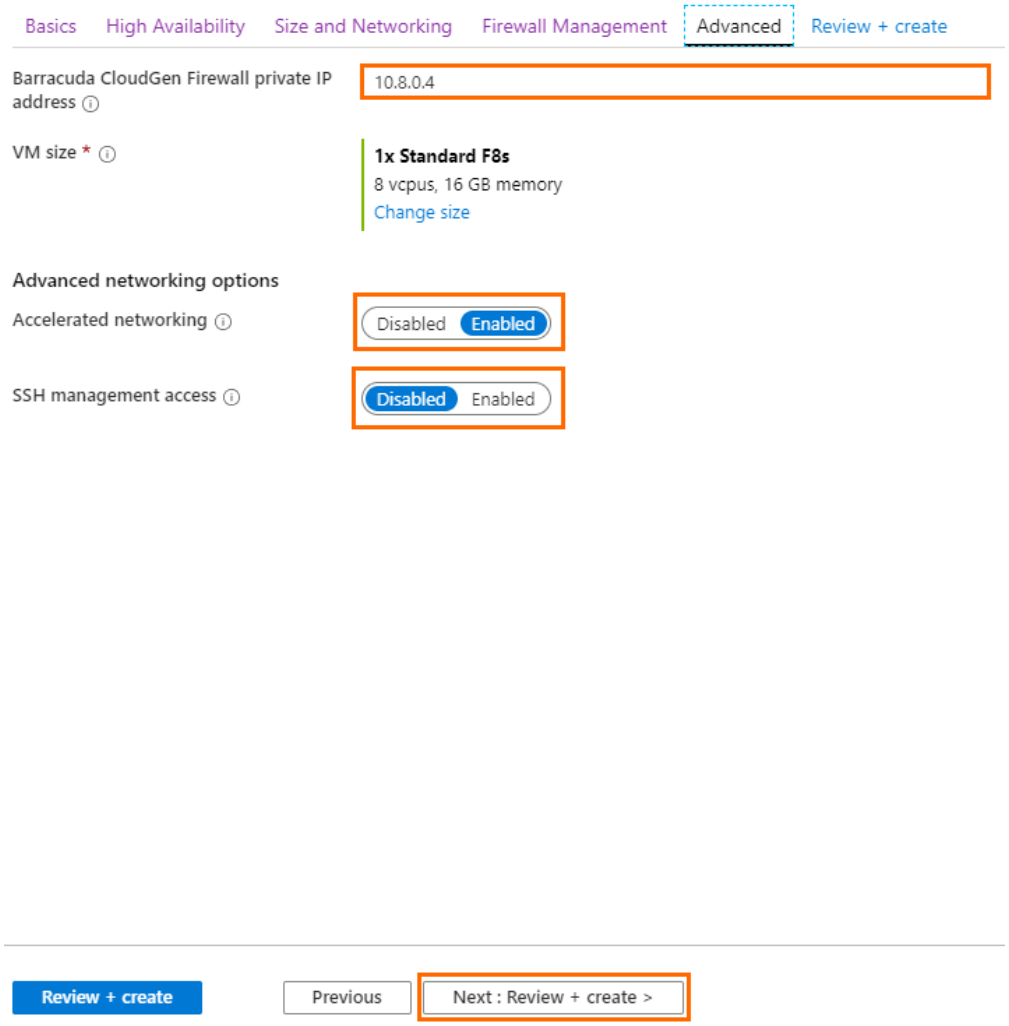


2. Click **Next : Advanced >**.

Step 5. Advanced

1. In the **Advanced** blade, configure the following settings.
   - **Barracuda CloudGen Firewall private IP address** – Enter a static private IP address from the subnet the firewall is deployed to. The first four and the last IP addresses in the subnet are reserved by Azure.
   - **VM size** – If not already configured, change the virtual machine size.
   - **Accelerated networking** – Enable or disable Azure Accelerated Networking if the size of your virtual machine meets the requirements of Microsoft.

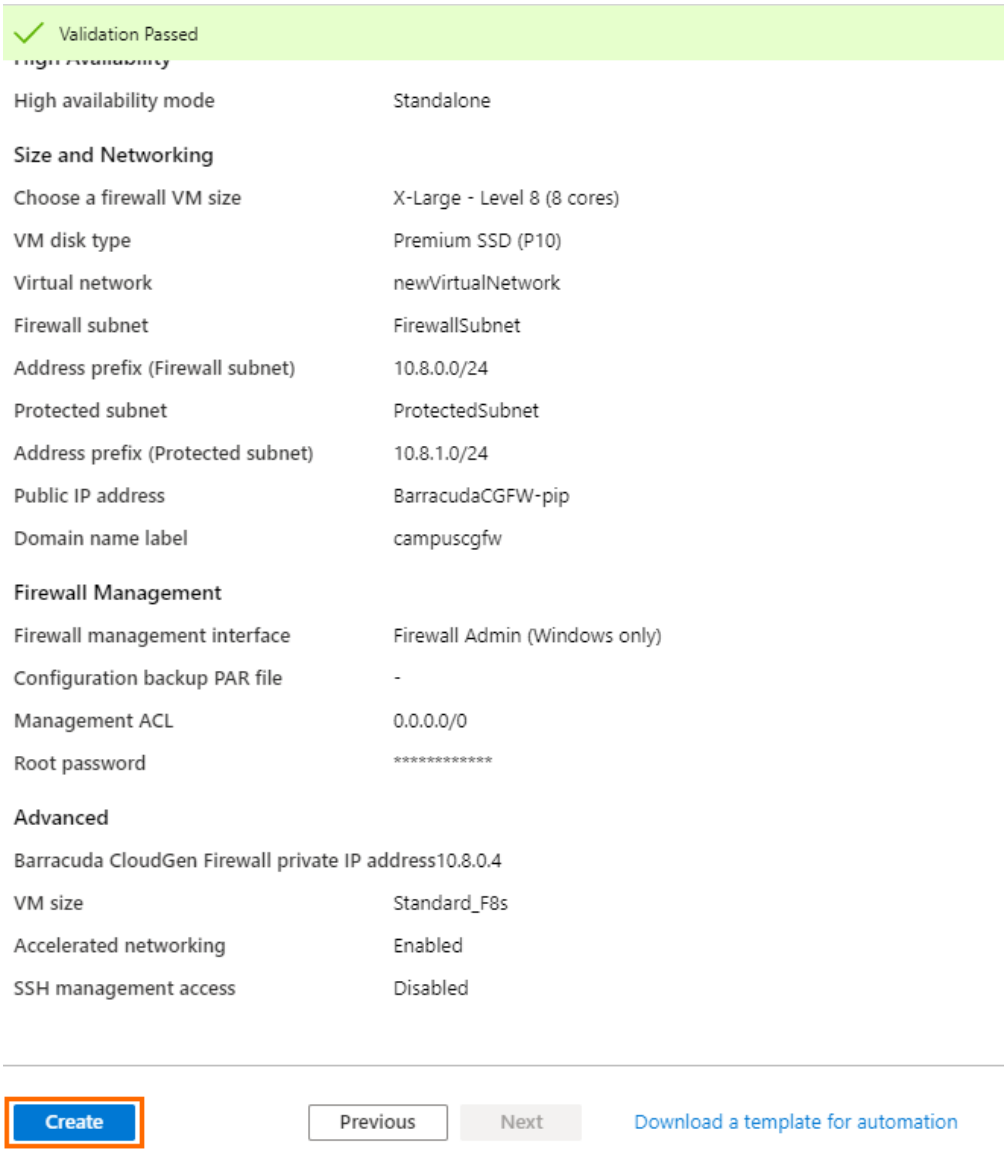
     Azure Accelerated Networking creates, for each existing interface, a second interface for Accelerated Networking (one for the hv_netvsc driver, and one for Mellanox). Use only every second interface in boxnet (e.g., eth0, eth2, eth4). On devices with DHCP enabled, eth0 is replaced with the DHCP interface. On DHCP-enabled devices, as well, use only every second interface (e.g. eth0, eth2, eth4).
   - **SSH management access** – Select **Enabled** to allow SSH access to the Barracuda CloudGen Firewall, and enter the **SSH public key**.



2. Click **Review + create >**.

Step 6. Summary

1. The basic configuration of the Barracuda CloudGen Firewall is validated, and if no errors are found, the virtual machine is ready for provisioning. For automated deployments, you can download the configuration template.



2. Click **Create** .
3. Wait for Microsoft Azure to finish the deployment of your Barracuda CloudGen Firewall.
4. Go to **Virtual machines** , click on the CloudGen Firewall VM, and locate the **Public IP address** used to connect to your firewall. Use this IP address to connect to your CloudGen Firewall, as configured, either via Barracuda Firewall Admin or Web User Interface. The username is **root** and the password is the password you configured in Step 4.

Next Steps

Configure a user-defined routing table for the backend VMs to send traffic through the firewall, and enable Azure Cloud Integration to allow the firewall VM to directly connect to the Azure service fabric.

Figures

1. market_place_search.png
2. market_create_cgf_sdwan.png
3. basic_blade.png
4. ha_blade.png
5. size_networking.png
6. mgmt.png
7. advanced.png
8. summary.png

© 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.