How to Deploy a CloudGen Firewall from the Microsoft Azure Market Place

https://campus.barracuda.com/doc/78157419/

If you are in a region, where the Azure Marketplace is not available, download VHD disk images from the Barracuda Download portal and deploy the firewall via user defined images.

For more information, see How to Upload Azure VHD Images for User Defined Images using ARM and How to Deploy a CloudGen Firewall in Microsoft Azure Using PowerShell and ARM.

The Barracuda CloudGen Firewall for Microsoft Azure can be deployed as a virtual machine in the Microsoft Azure cloud. The Azure Marketplace Template deploys a single firewall VM into a dedicated subnet of a new or existing Virtual Network and configures an Azure Route Table to use the firewall as the default gateway. For managed firewalls, the configuration is fetched from the Control Center.

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

- **Barracuda CloudGen Firewall (BYOL)** – These images use licenses purchased directly from Barracuda Networks. Barracuda Networks offers a 30-day evaluation license.
- **Barracuda CloudGen Firewall (PAYG)** – These images do not need to be licensed separately. Licensing fees are included in the hourly price of the blade. All charges are billed directly through your Microsoft Azure account.
- **Barracuda CloudGen Firewall Control Center (BYOL)** – These images use licenses purchased directly from Barracuda Networks. Barracuda Networks offers a 30-day evaluation license.

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

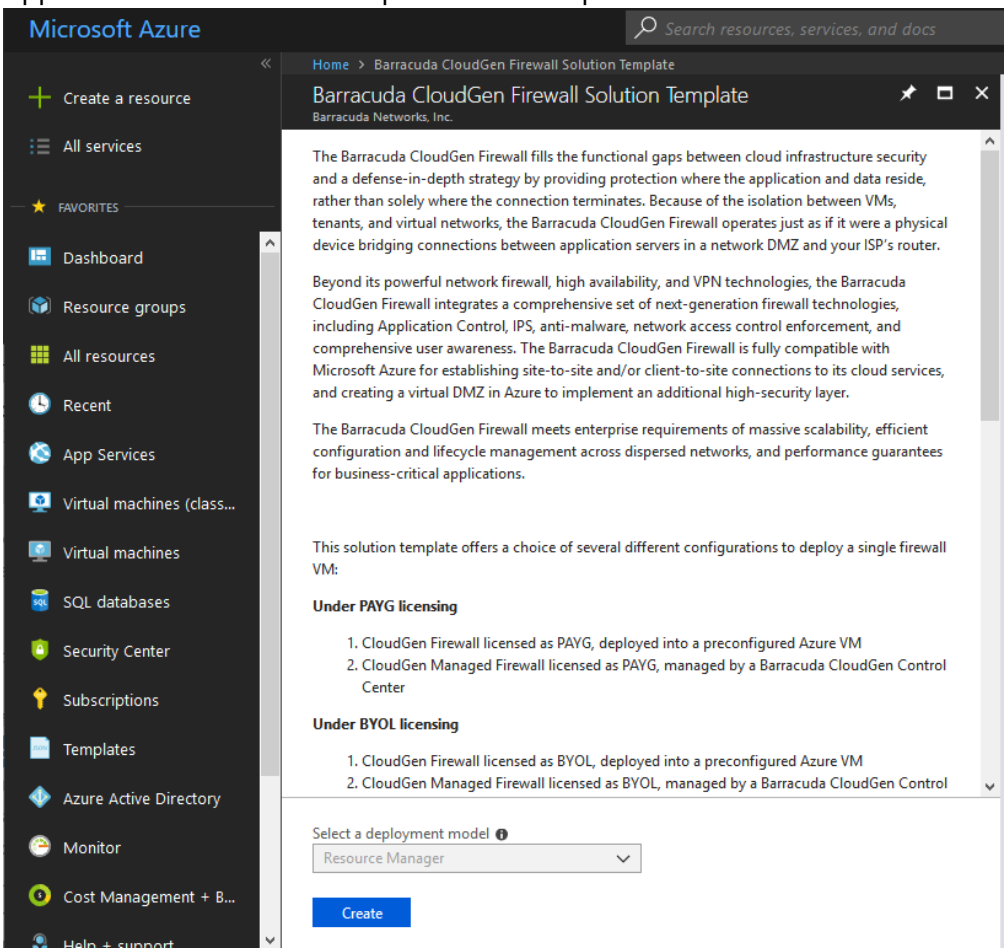
Before You Begin

- 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.

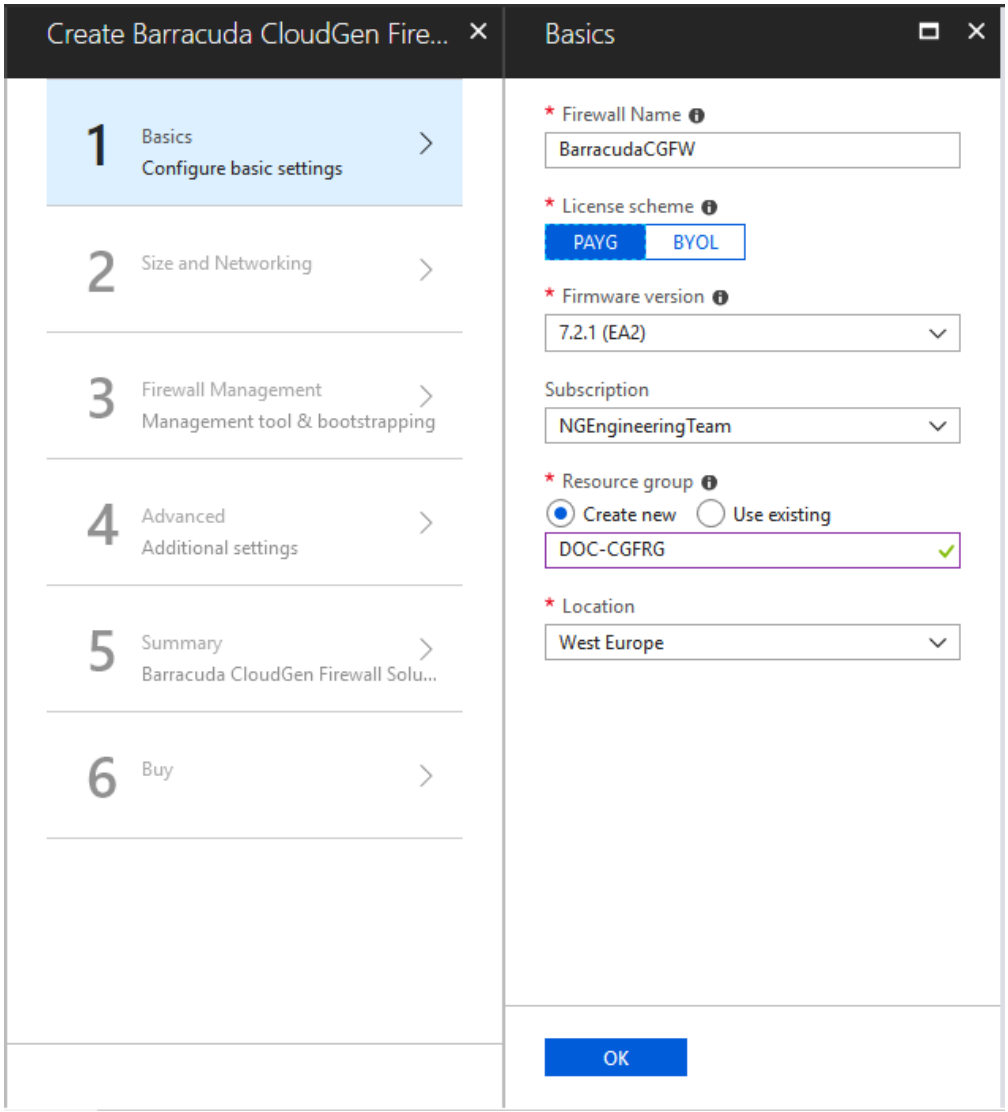
Step 1. Create a Resource

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` and select the CloudGen Firewall Single Appliance. The Solution Template window opens.



4. At the bottom of the window, click **Create**. The Barracuda CloudGen Firewall configuration opens.
5. In the **Basics** column, configure the following settings:
   - **Firewall Name** – Enter the name of the Barracuda CloudGen Firewall.
   - **License scheme** – Select the subscription image.
   - **Firmware version** – Select the firmware version of your firewall.
   - **Subscription** – Select the Azure Subscription.
   - **Resource group** – Enter a unique name for your resource group, or click **Use Existing** and select an existing resource group.
   - **Location** – Select the location of the firewall.

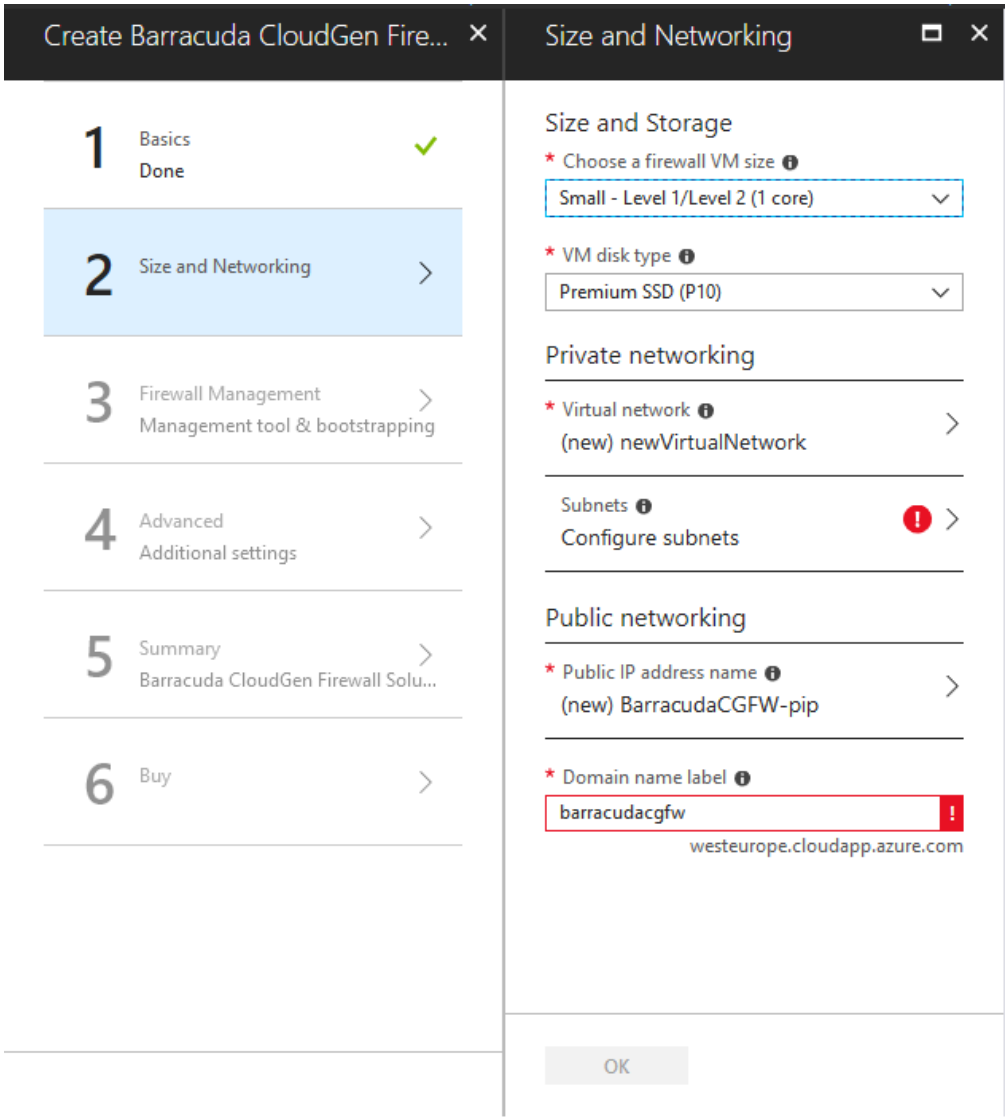


6. Click **OK**.

The Barracuda CloudGen Firewall configuration is now introduced and the **Size and Networking** configuration opens.

Step 2. Configure Network Settings

The recommended VM size the CloudGen Firewall should have according to your license is automatically selected. You can now create a virtual network, add a subnet, and assign a public IP address to the configuration.



Assign a Virtual Network

Assign a virtual network to your firewall. Use a large network not overlapping with your on-premise networks.

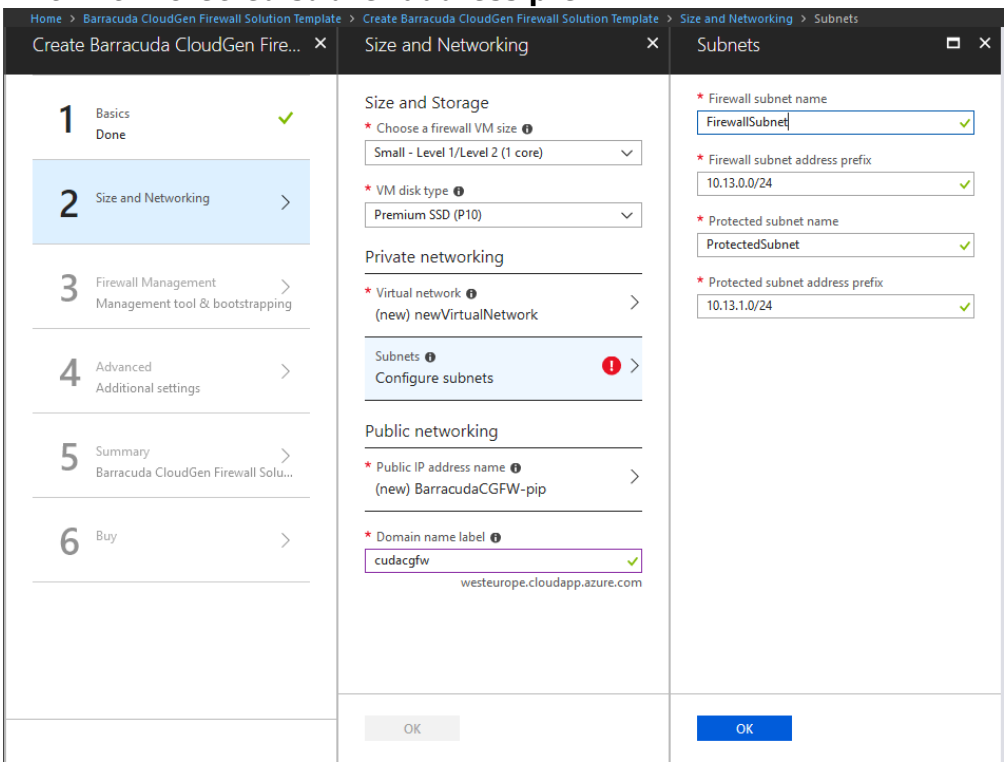
1. Click the expand-arrow on the right of the **Virtual network** field. The virtual network configuration opens.
2. Click **Create new** (**+**) (or select and existing virtual network.).
3. Enter a unique **Name** for the virtual network.
4. Enter the **Address space** of the virtual network.
5. Click **OK**.

Assign Subnets

Create one or more subnets. VMs behind the firewall should be deployed into a protected subnet. The

Firewall must be placed in a separate subnet from protected VMs.

1. Click the expand-arrow on the right of the **Subnets** field. The subnet configuration opens.
2. Click **Create new** (+) (or select and existing subnet.).
3. Enter a **Firewall subnet name** for the first subnet in the virtual network. E.g., `FirewallSubnet`. This subnet will be used to host the firewall.
4. Enter a **Firewall subnet address prefix**.
5. Enter a **Protected subnet name**. This subnet will be (re-)routed via the firewall.
6. Enter the **Protected subnet address prefix**.

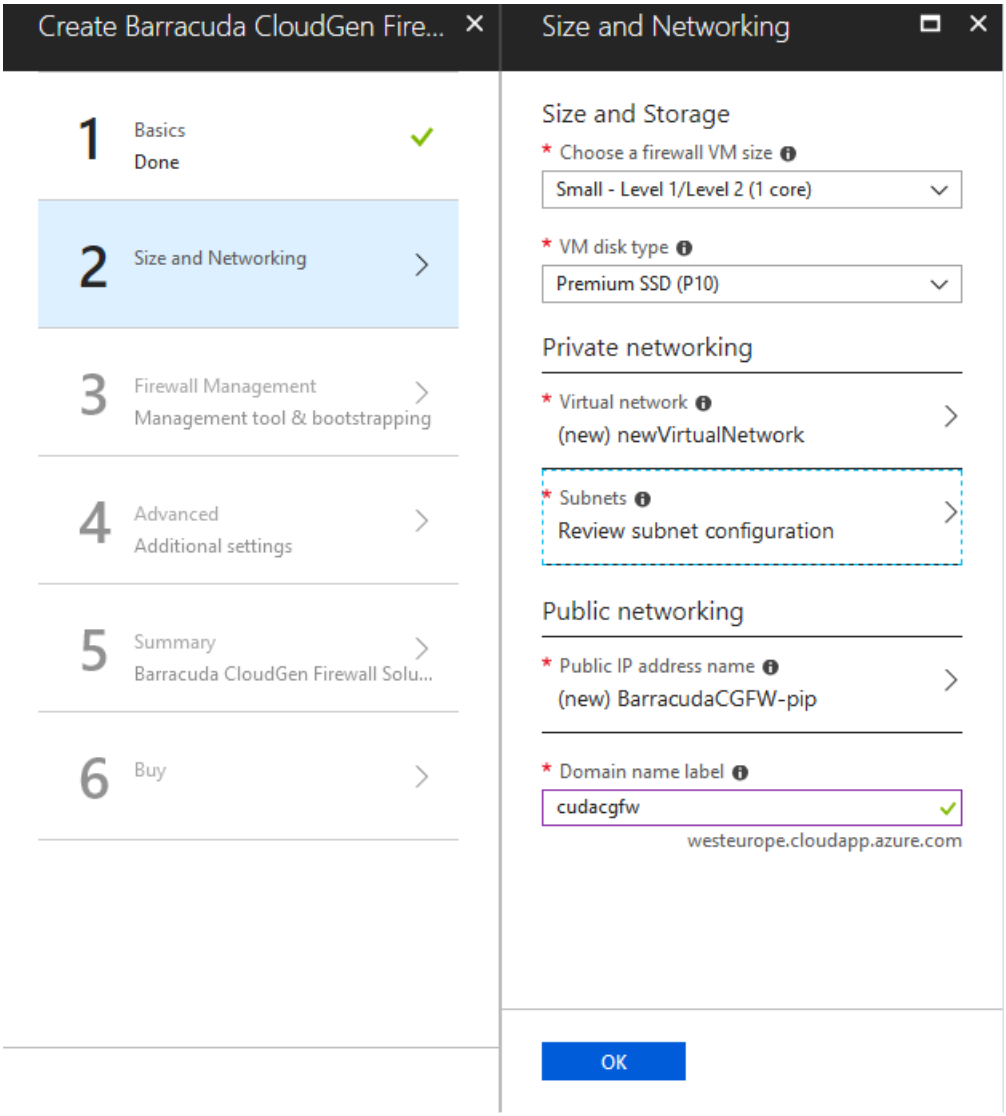


7. Click **OK**.

You can add additional protected subnets and associate them with the route table for them to send their traffic through the firewall.

Assign a Public IP Address

1. Click the expand-arrow on the right of the **Public IP address name** field. The public IP address configuration opens.
2. Click **Create new** (+).
3. Enter a **Name** for the public IP address resource.
4. Select the **SKU** for the public IP address.
   The SKU must match the SKU of the Load Balancer with which it is used.
5. Click **OK**.
6. In the **Domain name label** field, enter the prefix to use for the public IP address DNS name (e.g., [`prefix`].region.cloudapp.azure.com).



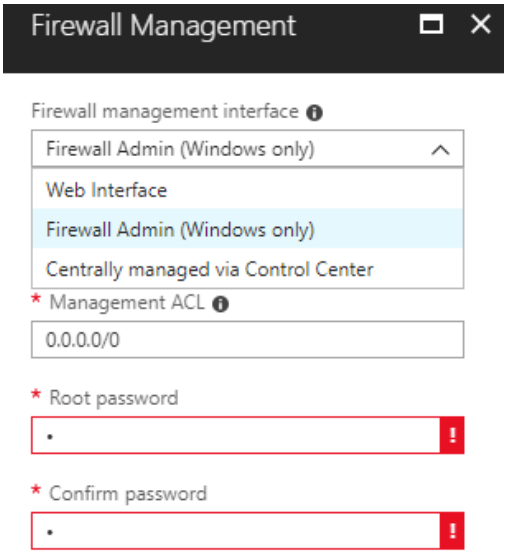
7. Click **OK**.

Your CloudGen Firewall does now have a virtual network, a subnet, and a Public IP address assigned.

Step 3. Configure Management Settings

Select how the CloudGen Firewall will be managed and configure authentication settings. Be aware that the Management ACL in this configuration is NOT the Management ACL configured on the CloudGen Firewall.

1. Select the **Firewall management interface**:



- **Web Interface** – The firewall is managed via web interface. For more information, see Web Interface.
  Configure the following settings:
  - **Management ACL** – Introduce an Azure Network Security Group to restrict access to management ports of the firewall. Enter `0.0.0.0/0` to allow access from any network.
  - **Root password** – Enter the root password required to access the CloudGen Firewall (min.: 6 characters).
- **Firewall Admin** – (Windows only) The firewall is managed via Barracuda Firewall Admin. For more information, see Barracuda Firewall Admin.
  Configure the following settings:
  - **Configuration backup PAR file** – Select an unencrypted configuration backup (PAR or PGZ) file of a Barracuda CloudGen Firewall to restore the configuration. For more information, see How to Back Up and Restore Firewall and Control Center Configurations.
    > If you are using static IP addresses in the firewall configuration, verify that the private IP address of the firewall VM is also used in the PAR file.
  - **Management ACL** – Introduce an Azure Network Security Group to restrict access to management ports of the firewall. Enter `0.0.0.0/0` to allow access from any network.
  - **Root password** – Enter the root password required to access the CloudGen Firewall (min.: 6 characters).
- **Centrally managed via Control Center** – The firewall is managed by a Control Center. For more information, see Firewall Control Center.
  Configure **Control Center binding**:
  1. Enter the publicly reachable **IP Address of the Control Center**. If the Control Center is behind another firewall, open port TCP 806.
  2. Enter the **Control Center Range ID** that contains the firewall configuration.
  3. Enter the **Control Center Cluster name** of the cluster that contains the firewall configuration.
  4. In the **PAR file retrieval key** field, enter the shared secret configured on the

Control Center to authenticate the firewall when retrieving the PAR file. On the firewall, go to **Box Properties > Operational** settings and enter the passphrase.

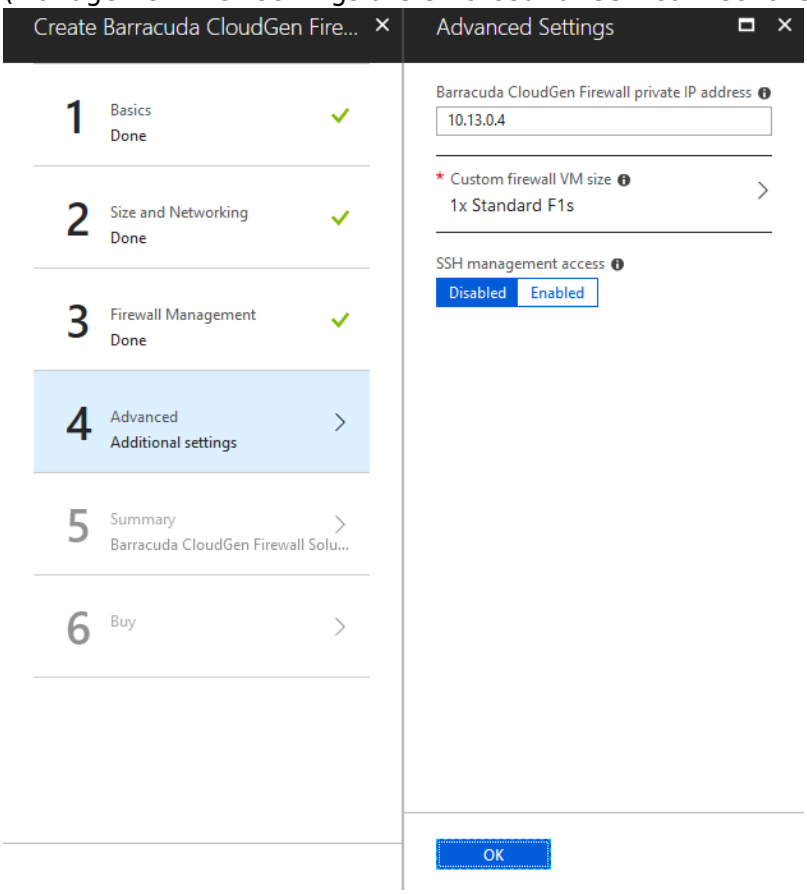
5. Click **OK**.

2. Click **OK**.

Step 4. (Optional) Configure Advanced Settings

Use this configuration to change IP address and size or to enable SSH access for the root user. The first four and the last IP addresses in the subnet are reserved by Azure.

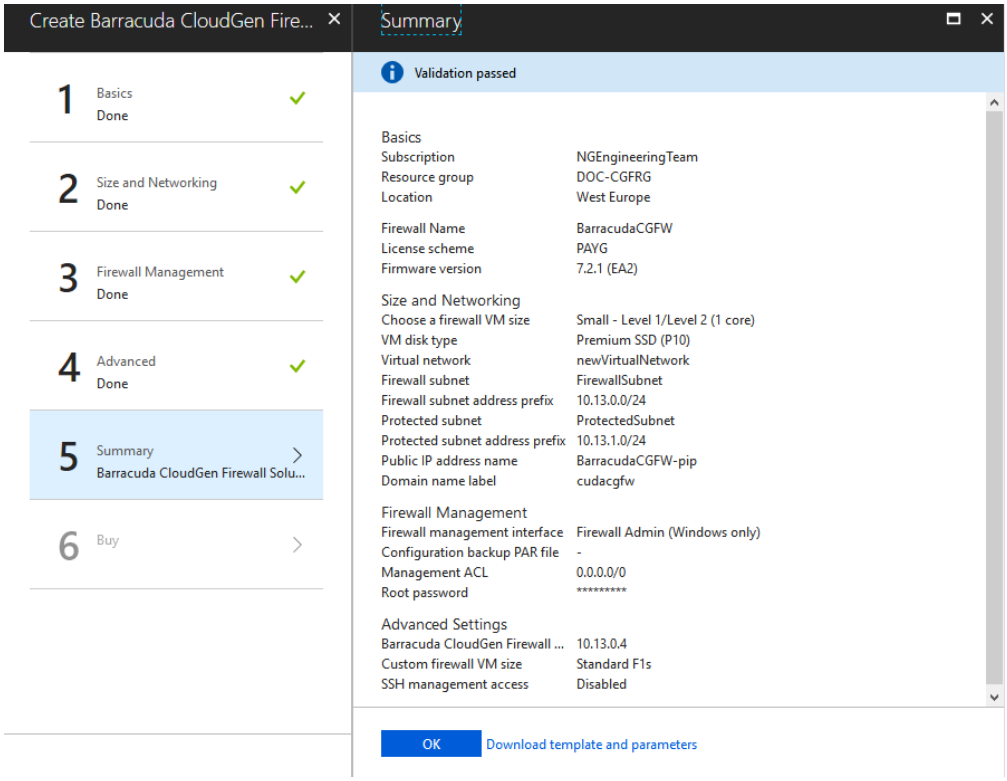
1. Change the **Barracuda CloudGen Firewall private IP address**. This must be a static IP address from the subnet the firewall is deployed to.
2. Override the **Custom Firewall VM size** selected in the **Size and Storage** configuration.
3. Enable **SSH management access** using key-based authentication for the root user. (Management ACL settings are enforced for SSH connections.)



4. Click **OK**.

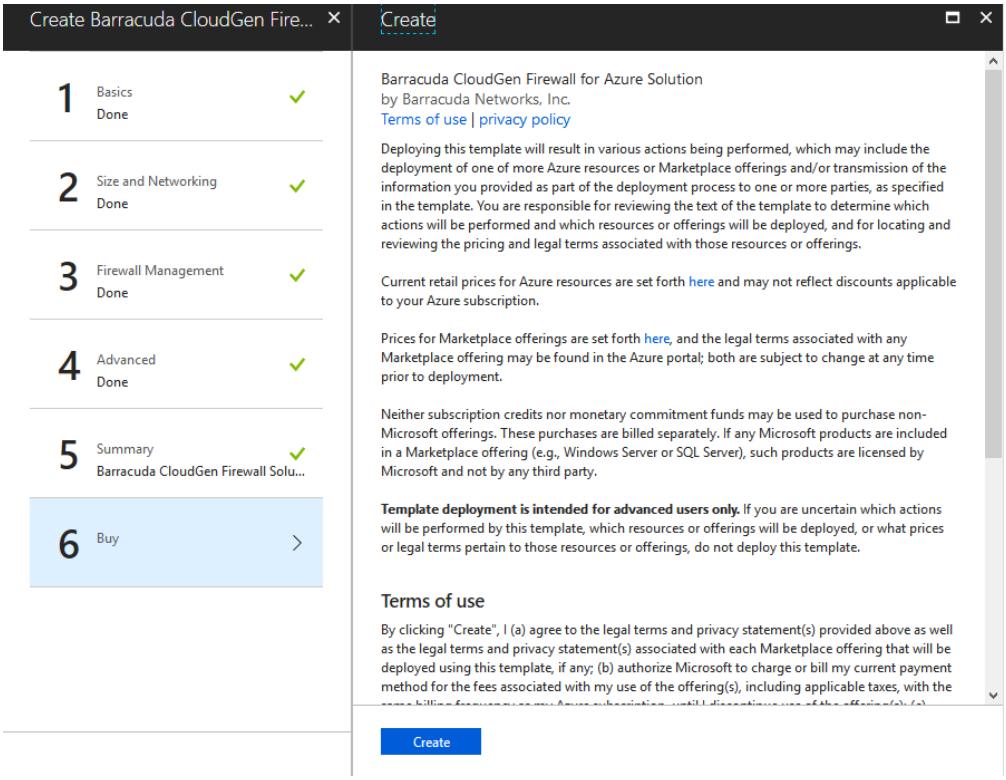
Step 5. Confirm the Purchase

After clicking **OK** the configuration gets validated and, if successful, presents the summary.



You can now purchase the firewall:

1. Click the **Download template and parameters** link at the bottom of the **Summary** window.
2. Click **OK**. The **Buy** window opens.



3. Enter your credentials in the required fields at the bottom of the Summary window.
4. Click **Create**.

Wait for Microsoft Azure to finish the deployment of your Barracuda CloudGen Firewall. Go to **Virtual machines**, click on the CloudGen Firewall VM, and locate the **Public IP address** used to connect to your firewall.

Open the public IP address with your browser for further links on how to download Barracuda Firewall Admin and how to receive an evaluation license.

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.

For more information, see How to Configure Azure Route Tables (UDR) using Azure Portal and ARM and How to Configure Azure Cloud Integration using ARM.

Figures

1. Image 001.png
2. Image 002.png
3. Image 003.png
4. Image 004.png
5. Image 005.png
6. Image 007.png
7. Image 009.png
8. Image 010.png
9. Image 011.png