

How to Deploy a Firewall Control Center from the Microsoft Azure Marketplace

<https://campus.barracuda.com/doc/96026617/>

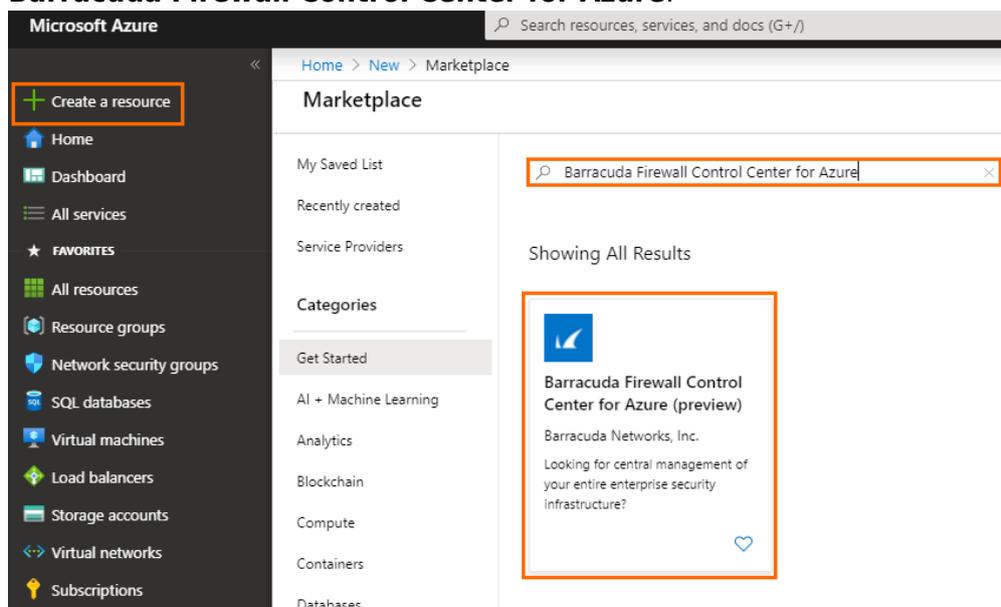
You can install the Firewall Control Center as a virtual machine in the Microsoft Azure public cloud. The Firewall Control Center is licensed using the Bring-Your-Own-License (BYOL) model. For more information, see [Firewall Control Center](#).

Before You Begin

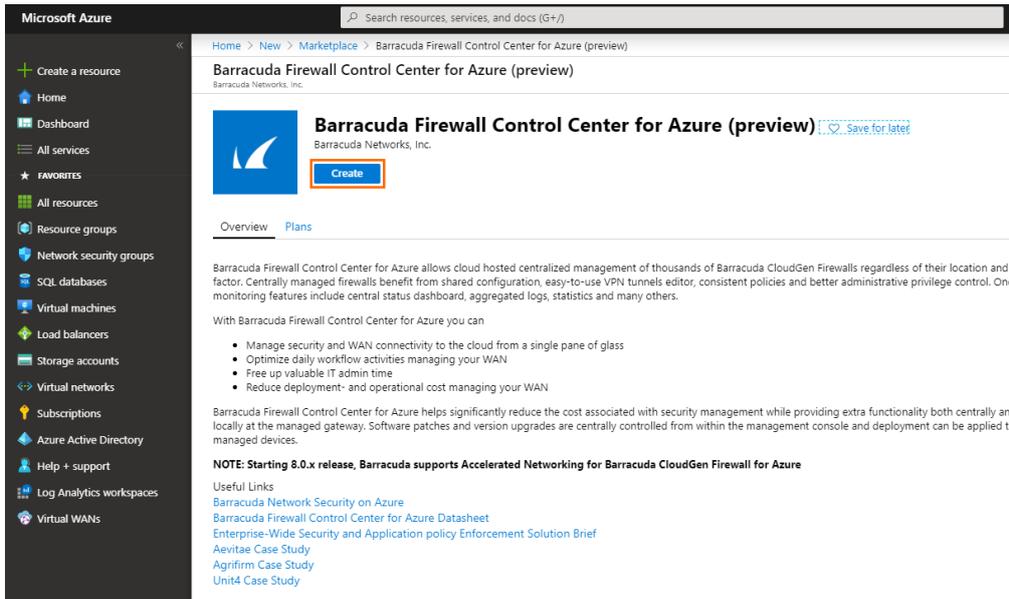
- Create a [Microsoft Azure account](#).
- Purchase a Firewall Control Center for Microsoft Azure license, or register to receive a 30-day evaluation license from the [Barracuda Networks Evaluation page](#).

Step 1. Basics

1. Go to the Azure portal: <https://portal.azure.com>
2. In the upper-left corner, click **+ Create a resource**.
3. Search the Marketplace for Barracuda Firewall Control Center for Azure and click **Barracuda Firewall Control Center for Azure**.



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



Microsoft Azure Search resources, services, and docs (G+)

Home > New > Marketplace > Barracuda Firewall Control Center for Azure (preview)

Barracuda Firewall Control Center for Azure (preview)

Barracuda Networks, Inc.



Barracuda Firewall Control Center for Azure (preview) Save for later

Create

Overview Plans

Barracuda Firewall Control Center for Azure allows cloud hosted centralized management of thousands of Barracuda CloudGen Firewalls regardless of their location and factor. Centrally managed firewalls benefit from shared configuration, easy-to-use VPN tunnels editor, consistent policies and better administrative privilege control. One monitoring features include central status dashboard, aggregated logs, statistics and many others.

With Barracuda Firewall Control Center for Azure you can

- Manage security and WAN connectivity to the cloud from a single pane of glass
- Optimize daily workflow activities managing your WAN
- Free up valuable IT admin time
- Reduce deployment- and operational cost managing your WAN

Barracuda Firewall Control Center for Azure helps significantly reduce the cost associated with security management while providing extra functionality both centrally and locally at the managed gateway. Software patches and version upgrades are centrally controlled from within the management console and deployment can be applied to managed devices.

NOTE: Starting 8.0.x release, Barracuda supports Accelerated Networking for Barracuda CloudGen Firewall for Azure

Useful Links

- [Barracuda Network Security on Azure](#)
- [Barracuda Firewall Control Center for Azure Datasheet](#)
- [Enterprise-Wide Security and Application policy Enforcement Solution Brief](#)
- [Aevitae Case Study](#)
- [Agrifirm Case Study](#)
- [Unit4 Case Study](#)

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 Control Center will be deployed to.
- **Control Center Name** – Enter the hostname for the Firewall Control Center.
- **Firmware version** – Select one of the available firmware versions. Barracuda Networks recommends deploying the highest available version.

Home > New > Marketplace > Barracuda Firewall Control Center for Azure (preview) > Create Barracuda Firewall Control Center for Azure

Create Barracuda Firewall Control Center for Azure

[Basics](#) [Networking](#) [Management](#) [Advanced](#) [Review + create](#)

The Barracuda CloudGen Firewall Control Center is a powerful, user-friendly appliance to manage your distributed network. As a Linux-based security appliance, there are a few differences between it and a typical server running on Azure:

- The Barracuda CloudGen Firewall Control Center Appliance administration is typically done with a Windows-based client application called as [Barracuda CloudGen Admin](#).
- This Barracuda CloudGen Firewall Control Center is licensed using the Bring-Your-Own-License (BYOL) model. [Fill out the evaluation form](#) to receive a 30-day evaluation license or purchase one of the licenses depending on your requirement.
- The Barracuda CloudGen Firewall Control Center for Azure is licensed for managing unlimited number of NextGen Firewall F gateways grouped in unlimited *clusters* and two *ranges*. Maximum capacity of a single Control Center virtual instance depends on instance size.

Note: The username to login to the appliance is **root** and the password is the one you have configured on Azure portal while deploying the VM. Also a forward for TCP/22, TCP/807, TCP/806 and TCP-UDP/692 endpoints will be created automatically when you deploy this VM. Click [here](#) for more details.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ	<input type="text" value="NGEngineeringTeam"/>
Resource group * ⓘ	<input type="text" value="(New) Campus_CC"/> Create new

Instance details

Region * ⓘ	<input type="text" value="West Europe"/>
Control Center Name * ⓘ	<input type="text" value="BarracudaCloudGenCC"/>
Firmware version * ⓘ	<input type="text" value="8.0.1"/>

[Review + create](#)

[Previous](#)

[Next : Networking >](#)

6. Click **Next : Networking >**.

Step 2. Networking

1. In the **Size and Networking** blade, configure the following settings:

- **Virtual network** – Select an existing **Virtual network**, or create a new one.
- **Control Center Subnet** – Select an existing subnet, or create a new one. This subnet will host your Control Center.
- **Public IP address name** – Select an existing **Public IP address**, or create a new one.

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 Control Center.

Home > New > Marketplace > Barracuda Firewall Control Center for Azure (preview) > Create Barracuda Firewall Control Center for Azure

Create Barracuda Firewall Control Center for Azure

Basics **Networking** Management Advanced Review + create

Private networking

Configure virtual networks

Virtual network * ⓘ

(new) CCNetwork

[Create new](#)

Control Center Subnet * ⓘ

(new) ControlCenterSubnet (10.16.0.0/24)

Public networking

Public IP address name * ⓘ

(new) BarracudaCloudGenCC-pip

[Create new](#)

Domain name label * ⓘ

campuscc

.westeurope.cloudapp.azure.com

Review + create

Previous

Next : Management >

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

Step 3. Management

1. In the **Management** blade, configure the following settings:

- **Management ACL** – Introduces a Network Security Group that restricts access to management ports of the Control Center. 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 Control Center.
- **Confirm password** – Retype the password for the **root** user of the Control Center.

[Home](#) > [New](#) > [Marketplace](#) > [Barracuda Firewall Control Center for Azure \(preview\)](#) > [Create Barracuda Firewall Control Center for Azure](#)

Create Barracuda Firewall Control Center for Azure

[Basics](#) [Networking](#) [Management](#) [Advanced](#) [Review + create](#)

Management ACL * ⓘ	<input type="text" value="0.0.0.0/0"/>
Root password * ⓘ	<input type="password" value="*****"/> ✓
Confirm password * ⓘ	<input type="password" value="*****"/> ✓

[Review + create](#)

[Previous](#)

[Next : Advanced >](#)

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

Step 4. Advanced

1. In the **Advanced** blade, configure the following settings:
 - **Private IP address** – Enter a static private IP address from the subnet the Control Center 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).

Basics Networking Management **Advanced** Review + create

Private IP address ⓘ

VM size * ⓘ
1x Standard DS2 v2
2 vcpus, 7 GB memory
[Change size](#)

Advanced networking options

Accelerated networking ⓘ Disabled Enabled

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

Step 5. Summary

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

[Home](#) > [New](#) > [Marketplace](#) > [Barracuda Firewall Control Center for Azure \(preview\)](#) > [Create Barracuda Firewall Control Center for Azure](#)

Create Barracuda Firewall Control Center for Azure

✓ Validation Passed

By clicking on this offering, you are accepting the terms of the offering, including the license, and you agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Basics

Subscription	NGEngineeringTeam
Resource group	Campus_CC
Region	West Europe
Control Center Name	BarracudaCloudGenCC
Firmware version	8.0.1

Networking

Virtual network	CCNetwork
Control Center Subnet	ControlCenterSubnet
Address prefix (Control Center Subnet)	10.16.0.0/24
Public IP address	BarracudaCloudGenCC-pip
Domain name label	campuscc

Management

Management ACL	0.0.0.0/0
Root password	*****

Advanced

Private IP address	10.16.0.4
VM size	Standard_DS2_v2
Accelerated networking	Enabled

[Create](#)

[Previous](#)

[Next](#)

[Download a template for automation](#)

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

Next Steps

- [Getting Started - Control Center for Microsoft Azure](#)

Figures

1. CC_marketplace.png
2. Create_CC.png
3. cc_basics.png
4. CC_network.png
5. cc_management.png
6. CC_advanced.png
7. CC_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.