How to Deploy a High Availability Cluster with Cloud Integration from the Microsoft Azure Marketplace

https://campus.barracuda.com/doc/96026618/

You can install the Barracuda CloudGen Firewall as a virtual machine in the Microsoft Azure public cloud. The Azure solution template deploys either a single firewall or a high availability cluster into a dedicated subnet of a new or existing virtual network. For more information on the deployment of a single firewall, see How to Deploy a CloudGen Firewall from the Microsoft Azure Marketplace. You can deploy a high availability cluster from the marketplace with Cloud Integration. In case of a failover, the Azure route table is rewritten to use the active firewall. Due to the limitation of Azure networking, all active sessions will time-out whenever a failover occurs. For more information on high availability and high availability in Azure, see High Availability and High Availability in Azure.

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.

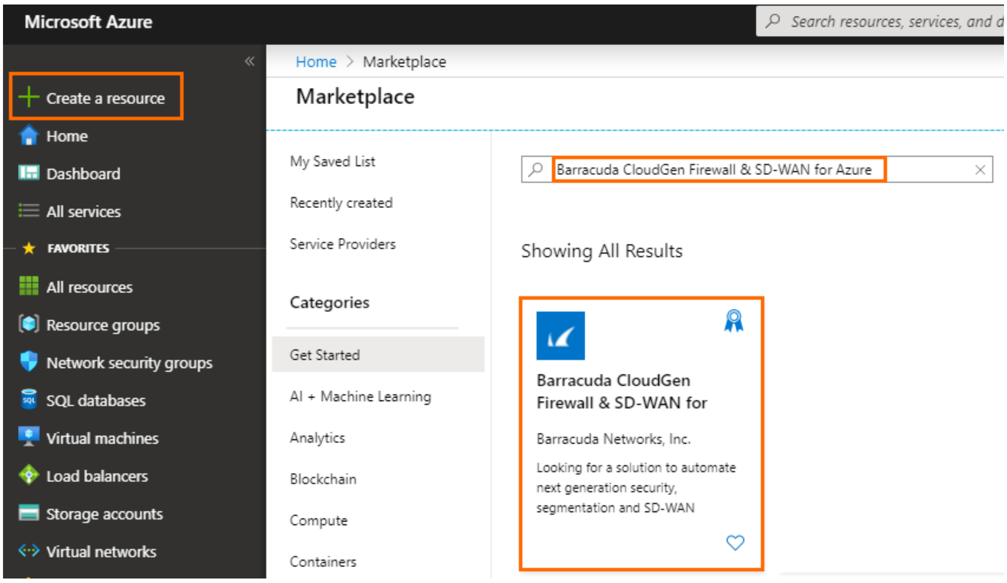
Before You Begin

- 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.

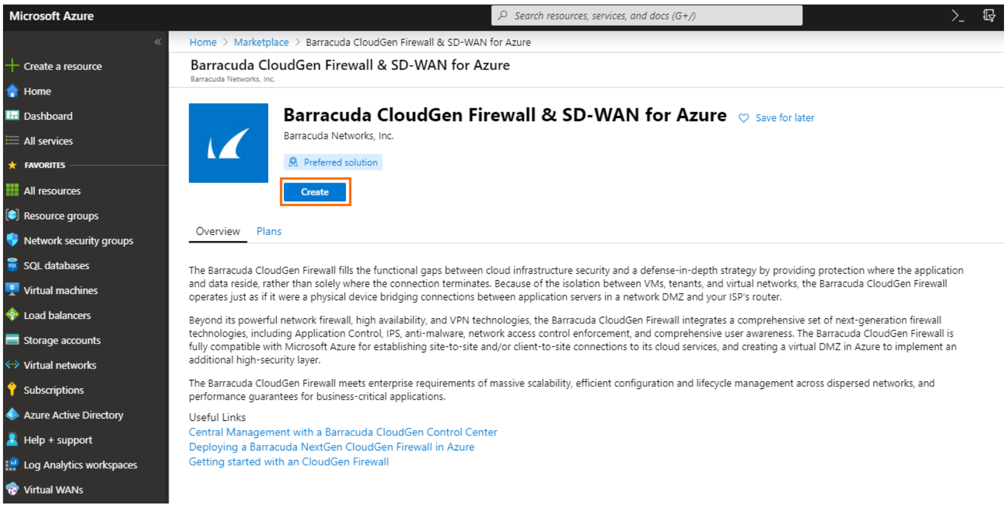
Deployment of the Firewall from Marketplace

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 CloudGen Firewall & SD-WAN for Azure` and click **Barracuda CloudGen Firewall & SD-WAN for Azure**.



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



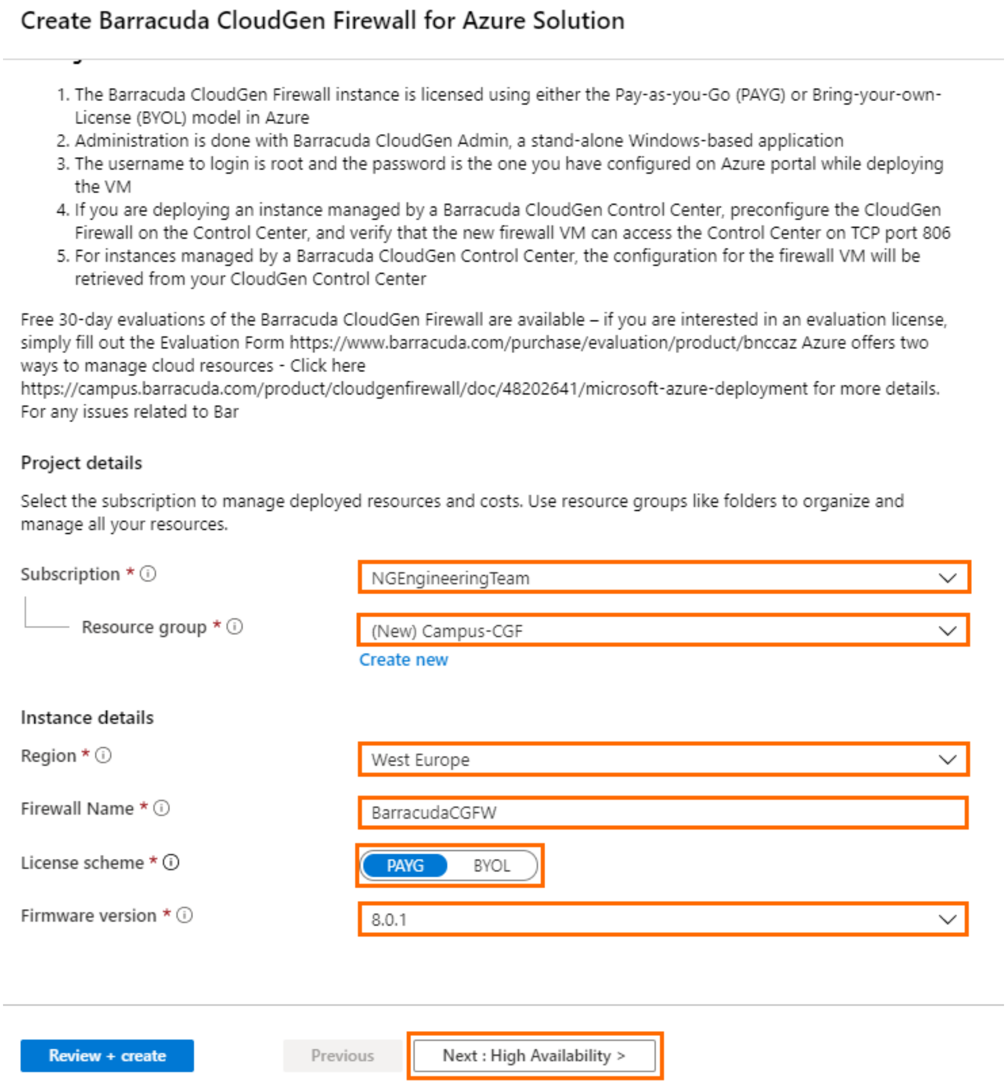
The Barracuda CloudGen Firewall fills the functional gaps between cloud infrastructure security and a defense-in-depth strategy by providing protection where the application and data reside, rather than solely where the connection terminates. Because of the isolation between VMs, tenants, and virtual networks, the Barracuda CloudGen Firewall operates just as if it were a physical device bridging connections between application servers in a network DMZ and your ISP's router.

Beyond its powerful network firewall, high availability, and VPN technologies, the Barracuda CloudGen Firewall integrates a comprehensive set of next-generation firewall technologies, including Application Control, IPS, anti-malware, network access control enforcement, and comprehensive user awareness. The Barracuda CloudGen Firewall is fully compatible with Microsoft Azure for establishing site-to-site and/or client-to-site connections to its cloud services, and creating a virtual DMZ in Azure to implement an additional high-security layer.

The Barracuda CloudGen Firewall meets enterprise requirements of massive scalability, efficient configuration and lifecycle management across dispersed networks, and performance guarantees for business-critical applications.

Useful Links
Central Management with a Barracuda CloudGen Control Center
Deploying a Barracuda NextGen CloudGen Firewall in Azure
Getting started with an CloudGen Firewall

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.



Create Barracuda CloudGen Firewall for Azure Solution

1. The Barracuda CloudGen Firewall instance is licensed using either the Pay-as-you-Go (PAYG) or Bring-your-own-License (BYOL) model in Azure
2. Administration is done with Barracuda CloudGen Admin, a stand-alone Windows-based application
3. The username to login is root and the password is the one you have configured on Azure portal while deploying the VM
4. If you are deploying an instance managed by a Barracuda CloudGen Control Center, preconfigure the CloudGen Firewall on the Control Center, and verify that the new firewall VM can access the Control Center on TCP port 806
5. For instances managed by a Barracuda CloudGen Control Center, the configuration for the firewall VM will be retrieved from your CloudGen Control Center

Free 30-day evaluations of the Barracuda CloudGen Firewall are available – if you are interested in an evaluation license, simply fill out the Evaluation Form https://www.barracuda.com/purchase/evaluation/product/bnccaz Azure offers two ways to manage cloud resources - Click here https://campus.barracuda.com/product/cloudgenfirewall/doc/48202641/microsoft-azure-deployment for more details. For any issues related to Bar

Project details

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

Subscription * ⓘ: NGEngineeringTeam

Resource group * ⓘ: (New) Campus-CGF

Instance details

Region * ⓘ: West Europe

Firewall Name * ⓘ: BarracudaCGFW

License scheme * ⓘ: [✓ PAYG] BYOL

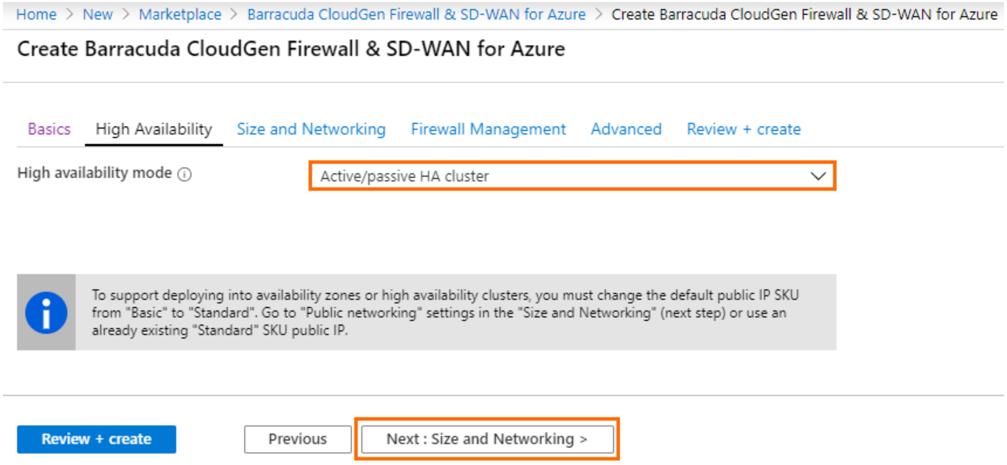
Firmware version * ⓘ: 8.0.1

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 **Active/passive HA cluster** from the drop-down menu.


Home > New > Marketplace > Barracuda CloudGen Firewall & SD-WAN for Azure > Create Barracuda CloudGen Firewall & SD-WAN for Azure
Basics
High Availability
Size and Networking
Firewall Management
Advanced
Review + create
Review + create
Previous
Next : Size and Networking >

Create Barracuda CloudGen Firewall & SD-WAN for Azure

High availability mode: Active/passive HA cluster

To support deploying into availability zones or high availability clusters, you must change the default public IP SKU from "Basic" to "Standard". Go to "Public networking" settings in the "Size and Networking" (next step) or use an already existing "Standard" SKU public IP.

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

If possible, the high availability cluster will be deployed into an availability zone. Otherwise, it will be deployed into an availability set.

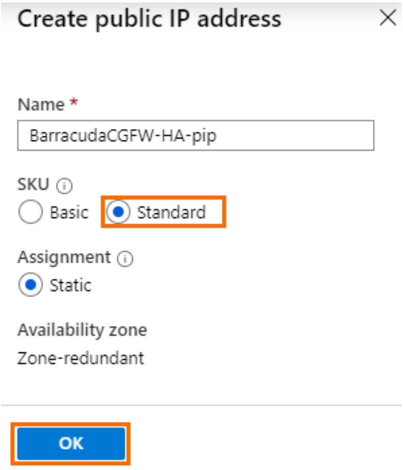
Step 3. Size and Networking

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.
   - **HA firewalls cluster subnet** – Select an existing subnet, or create a new one. This subnet will host your firewalls. The firewalls must be placed in a different subnet than the protected instances.
   - **Primary firewall's public IP address name** – Select an existing **Public IP address**, or create a new one.

     For a high availability cluster, you must select a **Standard** SKU public IP address. 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.

     To create a new public IP address, click **Create new** and select **Standard** SKU. Click **OK**.



Create public IP address

Name *
BarracudaCGFW-HA-pip

SKU
○ Basic ● Standard

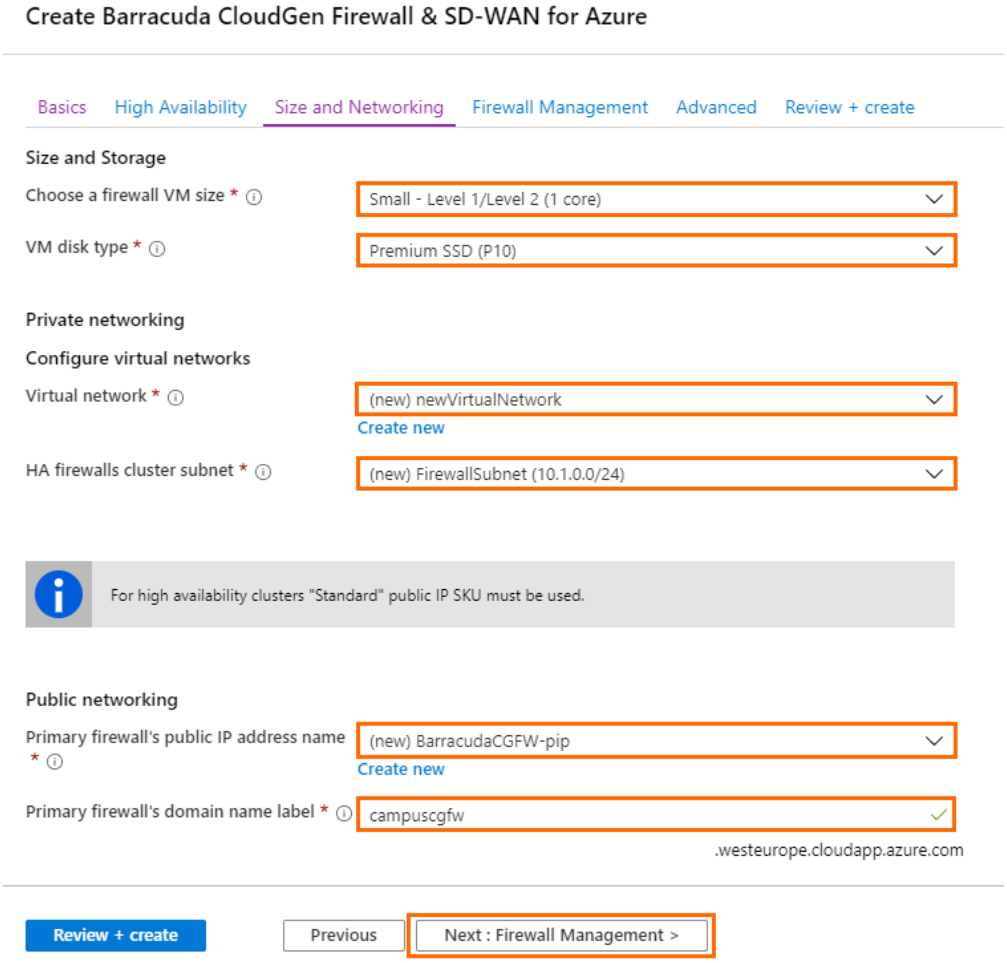
Assignment
● Static

Availability zone
Zone-redundant

- **Primary firewall's domain name label** – Enter a domain name for your primary firewall.
- **Secondary firewall's public IP address name** – Select an existing **Public IP address**, or create a new one.

  For a high availability cluster, you must select a **Standard** SKU public IP address.

  To create a new public IP address, click **Create new** and select **Standard** SKU. Click **OK**.
- **Secondary firewall's domain name label** – Enter a domain name for your secondary firewall.



Create Barracuda CloudGen Firewall & SD-WAN for Azure

Size and Storage

Choose a firewall VM size * : Small - Level 1/Level 2 (1 core)

VM disk type * : Premium SSD (P10)

Private networking

Configure virtual networks

Virtual network * : (new) newVirtualNetwork

HA firewalls cluster subnet * : (new) FirewallSubnet (10.1.0.0/24)

For high availability clusters "Standard" public IP SKU must be used.

Public networking

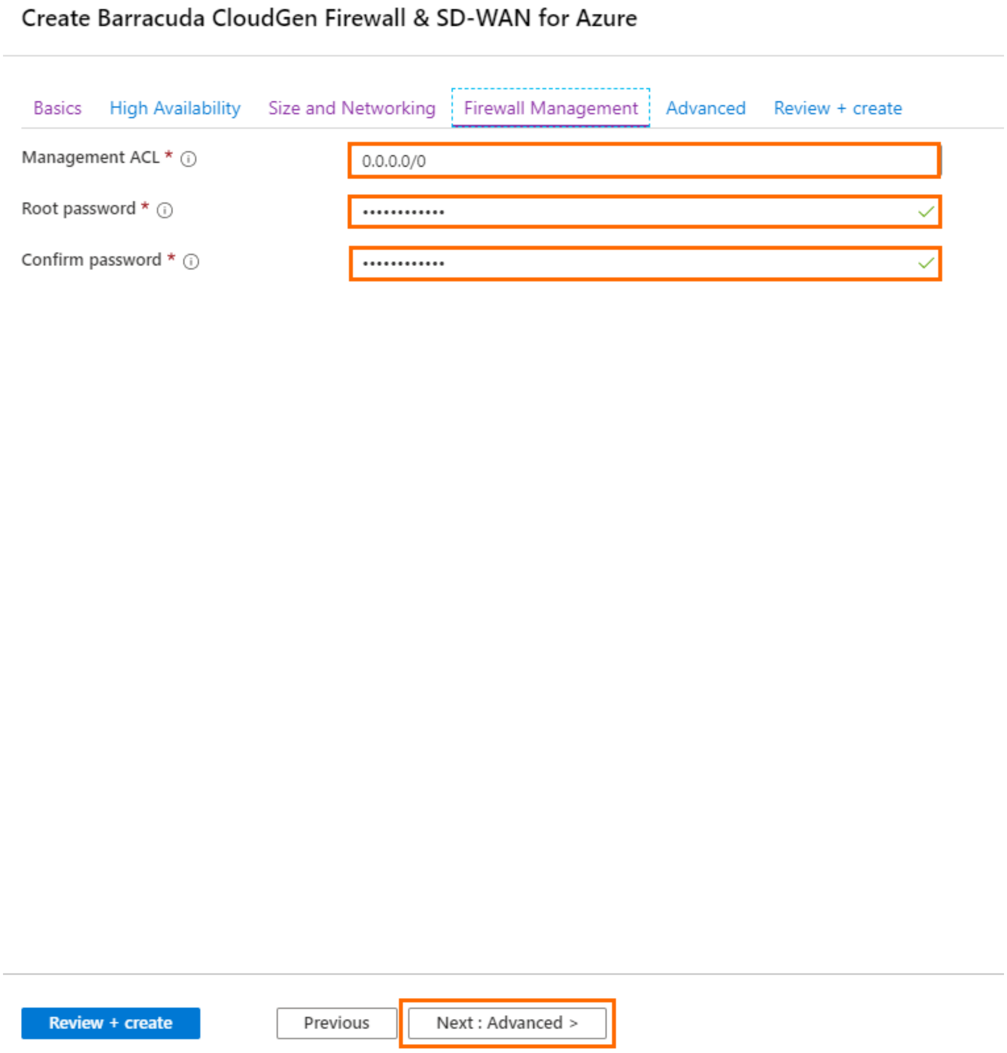
Primary firewall's public IP address name * : (new) BarracudaCGFW-pip

Primary firewall's domain name label * : campuscgfw
.westeurope.cloudapp.azure.com

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

Step 4. Firewall Management

1. In the **Firewall Management** blade, configure the following settings.
   - **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.



Create Barracuda CloudGen Firewall & SD-WAN for Azure

Management ACL * : 0.0.0.0/0

Root password * : ••••••••••••

Confirm password * : ••••••••••••

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

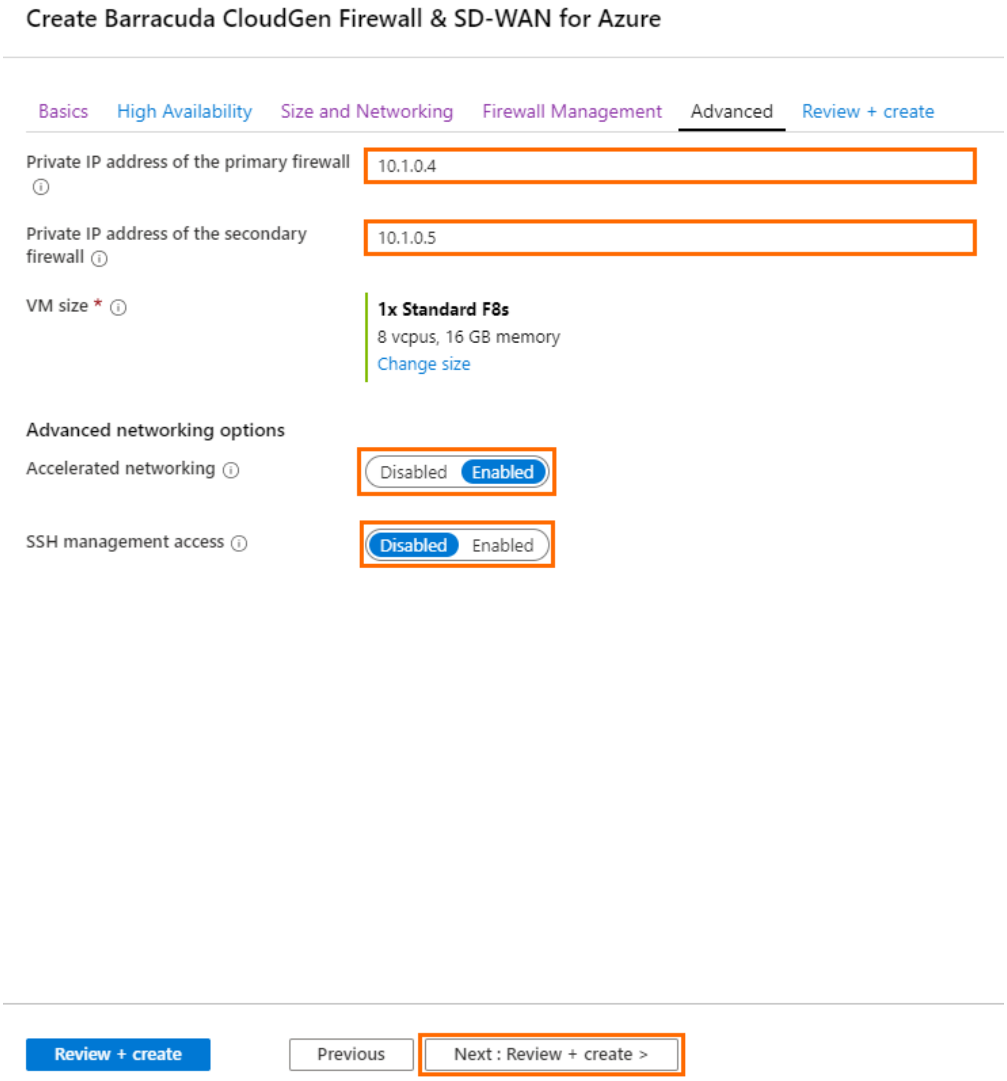
Step 5. Advanced

1. In the **Advanced** blade, configure the following settings.
   - **Private IP address of the primary firewall** – Enter a static private IP address from the subnet the firewalls are deployed to. The first four and the last IP addresses in the subnet are reserved by Azure.

- **Private IP address of the secondary firewall** – Enter a static private IP address from the subnet the firewalls are 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**.



Create Barracuda CloudGen Firewall & SD-WAN for Azure

Private IP address of the primary firewall: 10.1.0.4

Private IP address of the secondary firewall: 10.1.0.5

VM size *: 1x Standard F8s
8 vcpus, 16 GB memory

Advanced networking options

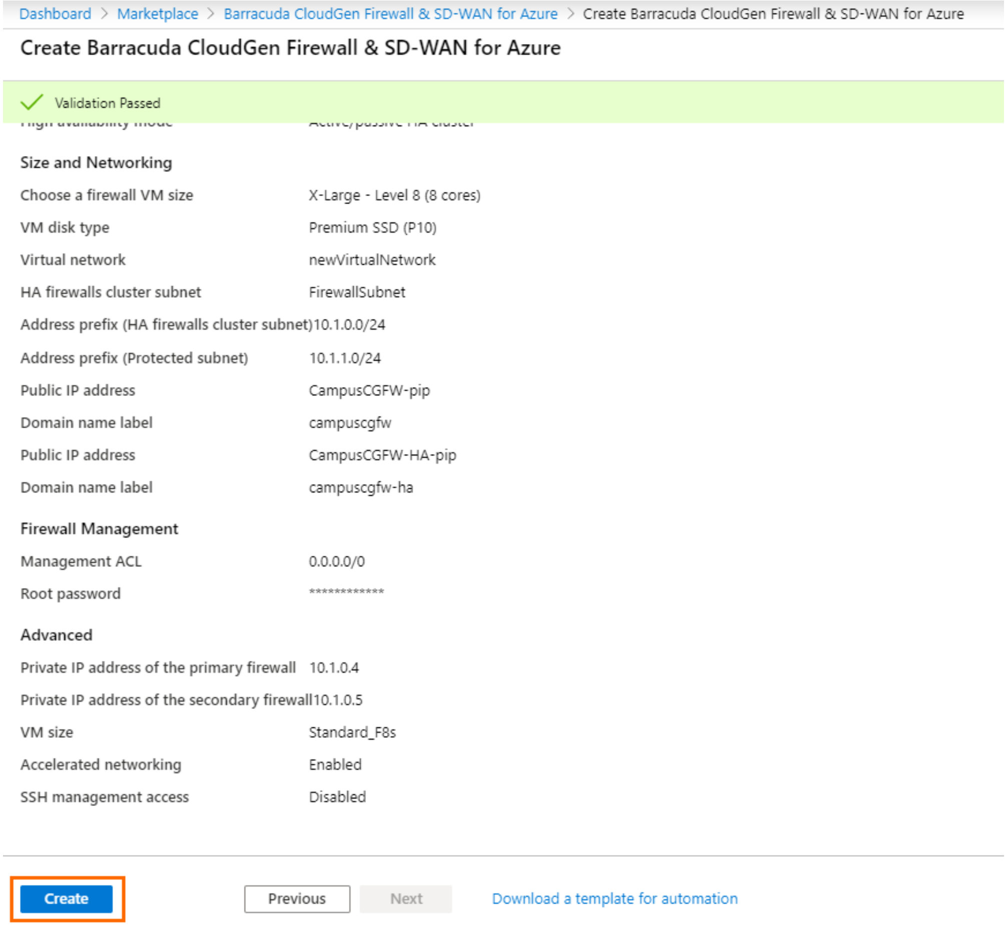
Accelerated networking: Disabled [✓ Enabled]

SSH management access: [✓ Disabled] Enabled

2. Click **Next : 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.



Dashboard > Marketplace > Barracuda CloudGen Firewall & SD-WAN for Azure > Create Barracuda CloudGen Firewall & SD-WAN for Azure

Create Barracuda CloudGen Firewall & SD-WAN for Azure

✓ Validation Passed

High availability mode	Active/passive HA cluster
Size and Networking	
Choose a firewall VM size	X-Large - Level 8 (8 cores)
VM disk type	Premium SSD (P10)
Virtual network	newVirtualNetwork
HA firewalls cluster subnet	FirewallSubnet
Address prefix (HA firewalls cluster subnet)	10.1.0.0/24
Address prefix (Protected subnet)	10.1.1.0/24
Public IP address	CampusCGFW-pip
Domain name label	campuscgfw
Public IP address	CampusCGFW-HA-pip
Domain name label	campuscgfw-ha
Firewall Management	
Management ACL	0.0.0.0/0
Root password	************
Advanced	
Private IP address of the primary firewall	10.1.0.4
Private IP address of the secondary firewall	10.1.0.5
VM size	Standard_F8s
Accelerated networking	Enabled
SSH management access	Disabled

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

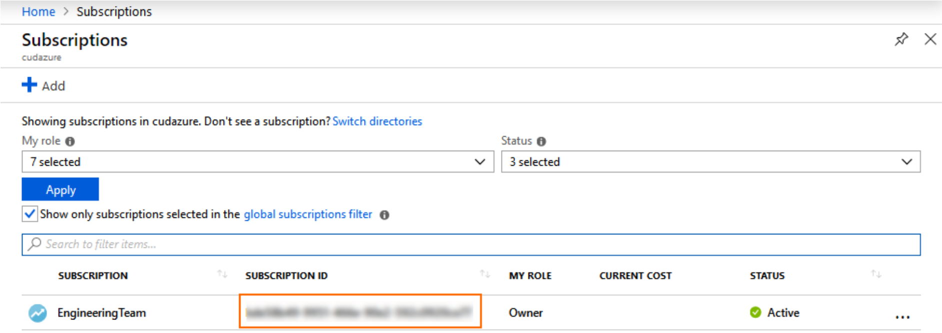
Configure Cloud Integration

Configure the Cloud Integration to automatically rewrite the Azure routing table in case of a failover to use the active firewall.

Step 1. Get Your Subscription ID

1. Log into the Azure portal: https://portal.azure.com

2. In the left menu, click **Subscriptions**.
3. Copy the **Subscription ID** in the **Subscription ID** column.



Home > Subscriptions

Subscriptions
cudazure

+ Add

Showing subscriptions in cudazure. Don't see a subscription? Switch directories

My role: 7 selected
Status: 3 selected

Apply

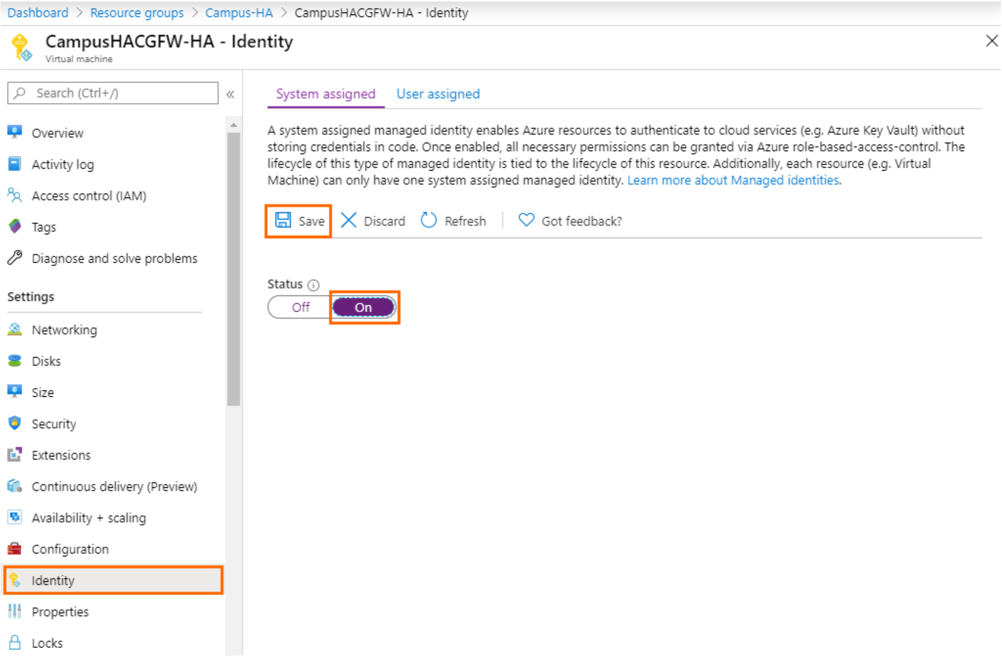
☑ Show only subscriptions selected in the global subscriptions filter

Search to filter items...

SUBSCRIPTION	SUBSCRIPTION ID	MY ROLE	CURRENT COST	STATUS
EngineeringTeam	[redacted]	Owner		Active

Step 2. Enable Managed Identities for Azure Resources

1. Go to the Azure portal: https://portal.azure.com.
2. Go to the resource group containing your high availability cluster.
3. Open the virtual machine of your primary firewall.
4. Click **Identity**.
5. Set **System assigned** to **On**.



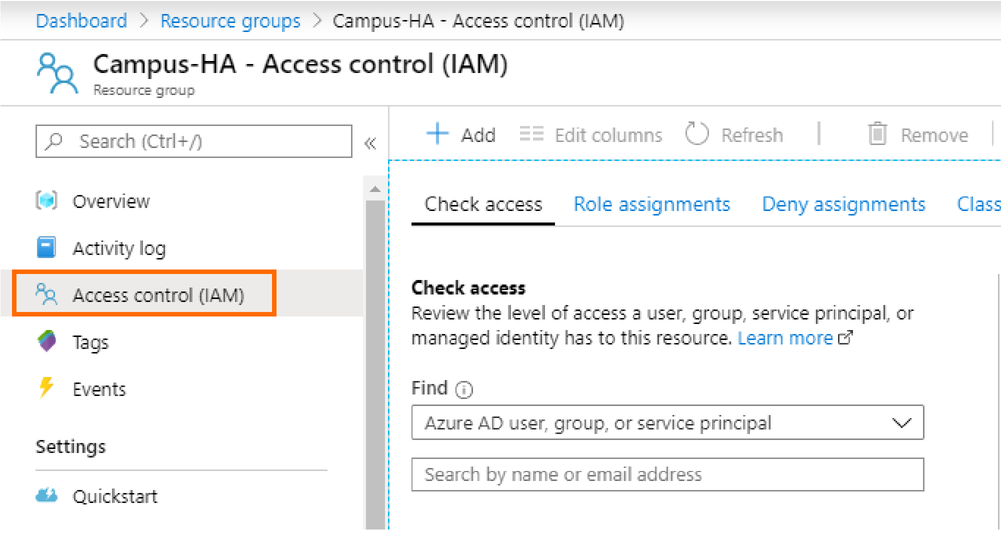
Dashboard > Resource groups > Campus-HA > CampusHACGFW-HA - Identity

CampusHACGFW-HA - Identity
Virtual machine

A system assigned managed identity enables Azure resources to authenticate to cloud services (e.g. Azure Key Vault) without storing credentials in code. Once enabled, all necessary permissions can be granted via Azure role-based-access-control. The lifecycle of this type of managed identity is tied to the lifecycle of this resource. Additionally, each resource (e.g. Virtual Machine) can only have one system assigned managed identity. Learn more about Managed identities.

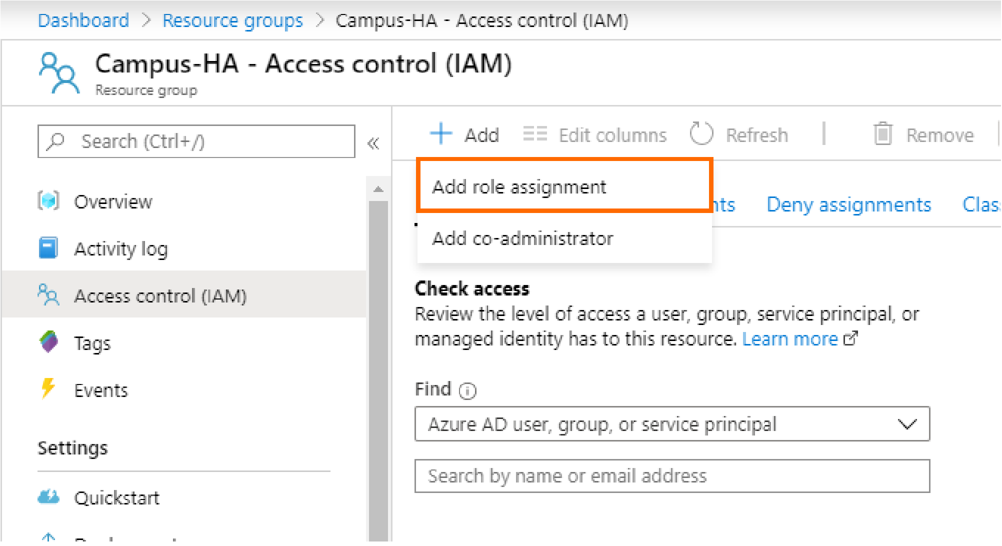
Status: Off [✓ On]

6. Click **Save**.
7. Open the virtual machine of your secondary firewall.
8. Click **Identity**.
9. Set **System assigned** to **On**.
10. Click **Save**.
11. Go to the resource group containing your high availability cluster.
12. Click **Access control (IAM)**.



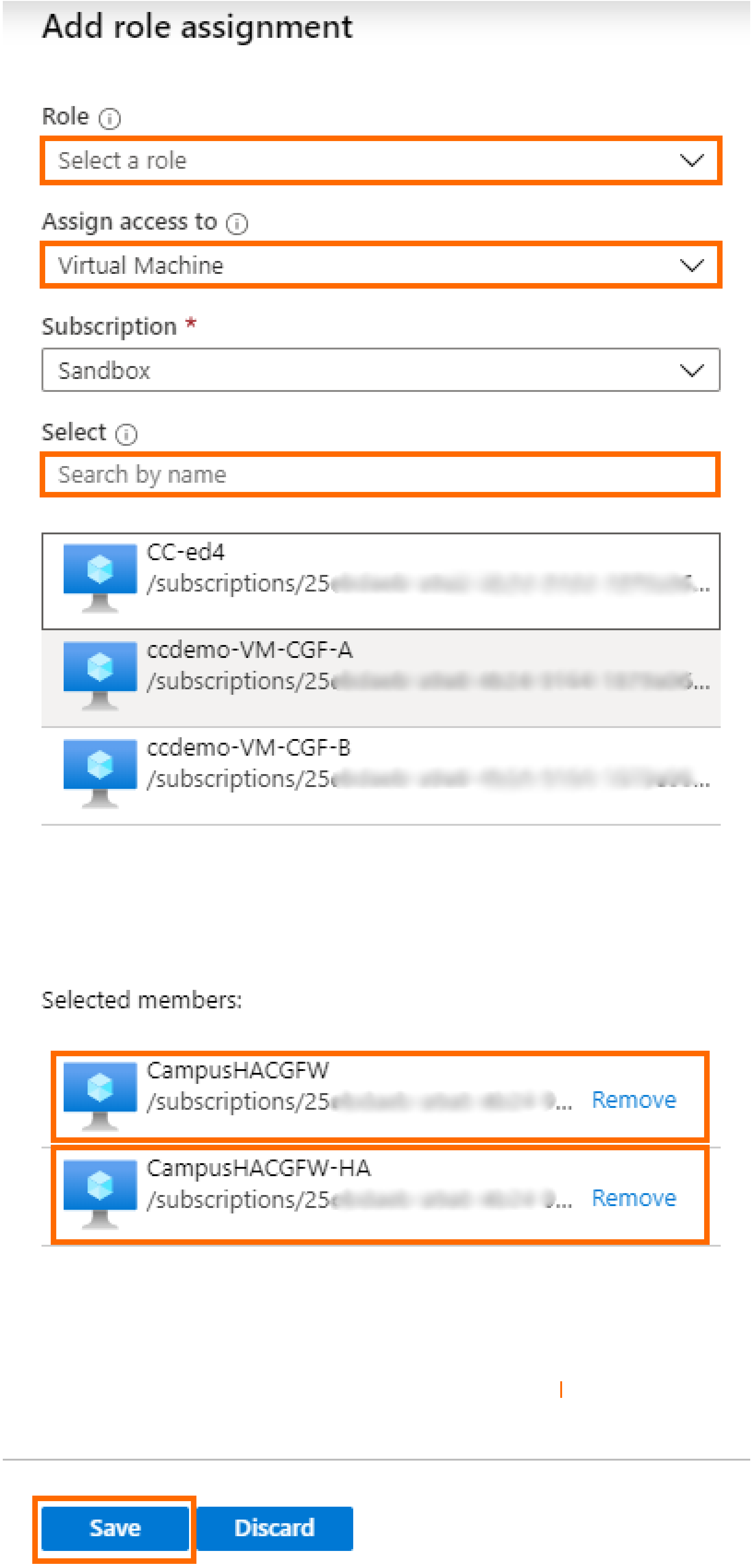
Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

13. Click **+Add** and click **Add role assignment**.



Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

14. For **Role**, select **Contributor** from the list.
15. For **Assign access to**, select **Virtual Machine** from the list.
16. For **Select**, enter the name of the primary firewall and click on the corresponding entry.
17. Click in the **Select** field again.
18. Enter the name of the secondary firewall, and click on the corresponding entry.
19. Click **Save**.



Add role assignment

Role: Select a role

Assign access to: Virtual Machine

Subscription *: Sandbox

Select: Search by name

CC-ed4
/subscriptions/25[redacted]...

ccdemo-VM-CGF-A
/subscriptions/25[redacted]...

ccdemo-VM-CGF-B
/subscriptions/25[redacted]...

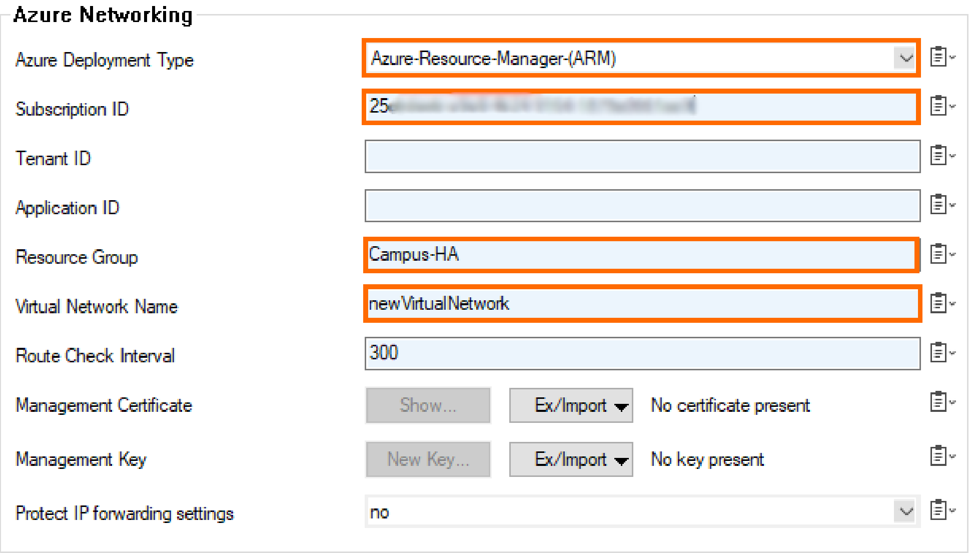
Selected members:

CampusHACGFW
/subscriptions/25[redacted]... Remove

CampusHACGFW-HA
/subscriptions/25[redacted]... Remove

Step 3. Configure Cloud Integration on Your CloudGen Firewall

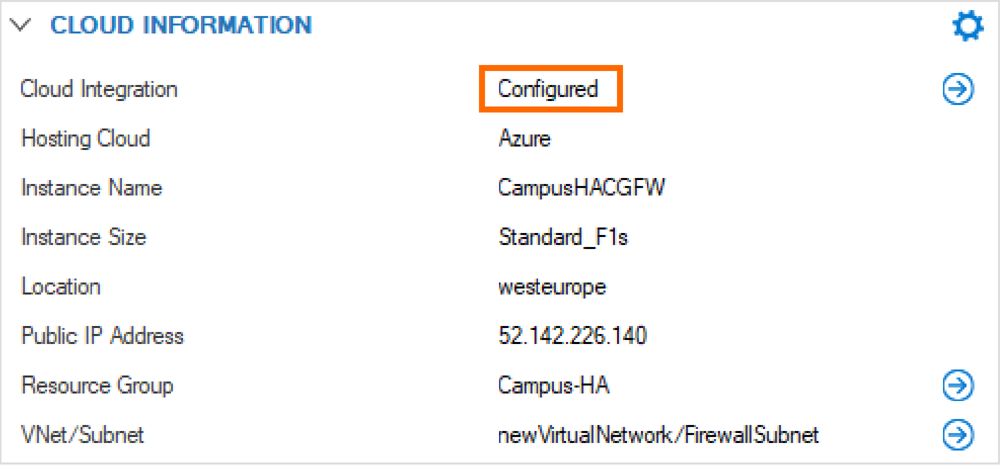
1. Locate the public IP address of the virtual machine of your primary firewall in Azure.
2. Log into the primary firewall of your high availability cluster with user **root**. For the password, see Step 4 of the deployment.
3. Go to **CONFIGURATION > Configuration Tree > Advanced Configuration > Cloud Integration**.
4. On the left side, click **Azure Networking**.
5. Click **Lock**.
6. In the **Azure Networking** section, specify values for the following:
    - **Azure Deployment Type** – Select **Azure Resource-Manager-(ARM)** from the drop-down menu.
    - **Subscription ID** – Enter your subscription ID.
    - **Resource Group** – Enter the name of the resource group containing the high availability cluster.
    - **Virtual Network** – Enter the name of the virtual network the high availability cluster is attached to.



Azure Networking

Azure Deployment Type	Azure-Resource-Manager-(ARM)	
Subscription ID	25[redacted]	
Tenant ID		
Application ID		
Resource Group	Campus-HA	
Virtual Network Name	newVirtualNetwork	
Route Check Interval	300	
Management Certificate	Show... Ex/Import	No certificate present
Management Key	New Key... Ex/Import	No key present
Protect IP forwarding settings	no	

7. Click **Send Changes** and **Activate**.
8. (Optional) Go to **DASHBOARD** and verify that **Cloud Integration** is **Configured** in the **CLOUD INFORMATION** section.



CLOUD INFORMATION

Cloud Integration	Configured
Hosting Cloud	Azure
Instance Name	CampusHACGFW
Instance Size	Standard_F1s
Location	westeurope
Public IP Address	52.142.226.140
Resource Group	Campus-HA
VNet/Subnet	newVirtualNetwork/FirewallSubnet

Next Steps

Configure a user-defined routing table for the backend VMs to send traffic through the firewall.

Figures

© 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.