Microsoft Azure Deployment

https://campus.barracuda.com/doc/73719655/

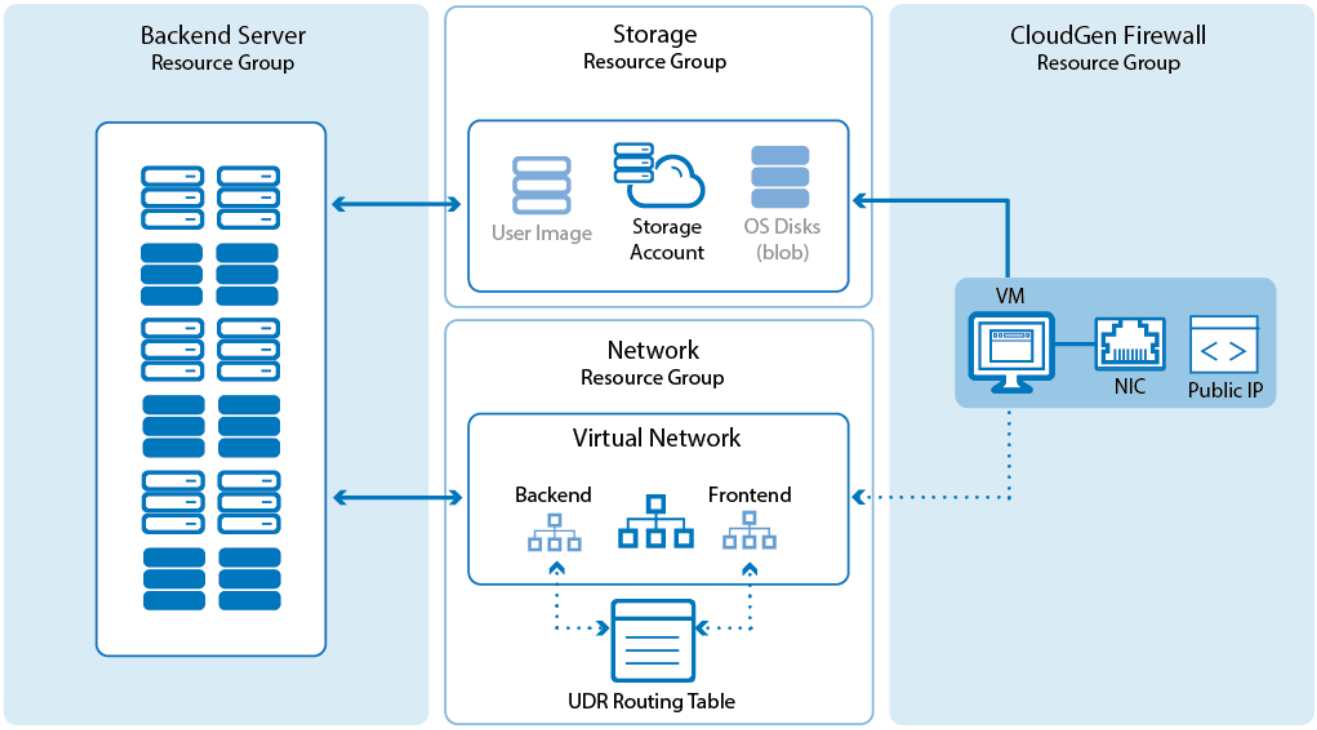
To deploy the Barracuda CloudGen Firewall on Microsoft Azure, use the Azure Resource Manager. Grouping your resources into resource groups makes it easy to create modular setups.

There are several different configuration and deployment tools available for an Azure cloud deployment:

- Web Portal (https://portal.azure.com)
- Azure Templates
- Azure Cloud Shell (Bash and PowerShell)
- REST API
- Azure CLI

Not all configuration tools offer the same functionality. Please refer to the Microsoft Azure product documentation for more information.

Azure Resource Manager Deployment



In the Azure Resource Manager deployment model, each resource is placed in a resource group.

These logic containers allow you to group your resources to simplify monitoring and to access control and billing for your applications. Resource groups also make it easier to re-deploy individual parts. For example, if you need to update the application servers, you only redeploy the resource group for these VMs, leaving the rest untouched.

Deployment of a CloudGen Firewall or Control Center via Azure Portal

The Azure portal allows you to deploy the Barracuda CloudGen Firewall and Firewall Control Center images from the Azure Marketplace using an easy-to-use web interface. Azure solution templates allow you to deploy one of the multiple preconfigured solutions depending on your use case in Azure.

For more information, see How to Deploy a CloudGen Firewall from the Microsoft Azure Market Place, How to Deploy a High Availability Cluster with Cloud Integration from the Microsoft Azure Marketplace and How to Deploy a Firewall Control Center from the Microsoft Azure Marketplace .

Deployment of a CloudGen Firewall or Control Center via Azure PowerShell

For custom deployments using user images, or other Azure features not available via the web portal, use Azure PowerShell to deploy your firewall VM.

For more information, see How to Deploy a CloudGen Firewall in Microsoft Azure Using PowerShell and ARM.

Deployment of a CloudGen Firewall or Control Center via Azure Templates

Azure templates are JSON files containing resource descriptions and parameter definitions. These parameters can be passed to the template during deployment either on the command line or through a template file. Deploy templates using Cloud Shell (PowerShell, Bash), Azure Rest API, or Visual Studio.

- Templates can be up to 1 MB in size. Parameter files up to 64 KB.
- Azure PowerShell 1.0 or higher is required.
- You can only deploy resources in one Azure location per template.

Templates can be deployed in two modes: incremental and complete. Neither deployment mode re-deploys existing resources in the resource group, as long as the configuration settings in the template are identical to the running resource. Resources defined in the template that are missing in the

resource group are added. The difference between the two modes is how resources not part of the template, but already running in the resource group, are handled. In incremental mode, these resources are left unchanged, whereas in complete mode these resources are deleted. Production deployments should use complete mode to secure against rogue configuration elements. Incremental mode should be used during template development. It should also be used in cases where either a resource cannot be created with the template or should not be managed by the template.

For more information, see How to Deploy a CloudGen Firewall via Azure Templates.

Modifying a CloudGen Firewall Azure Template to Retrieve the PAR File

If you are using the Firewall Control Center either on-premises or in the cloud, modify the Azure template to retrieve the PAR file for the new CloudGen Firewall VM directly from the Control Center during deployment. The scripts authenticate either with CC admin credentials or a shared secret.

For more information, see How to Modify Azure Templates to Retrieve the PAR File from a Control Center.

Deploy a CloudGen Firewall High Availability Cluster

To avoid downtime when the primary firewall is unavailable due to maintenance or hardware failure, configure a high availability cluster. A Microsoft Azure Load Balancer in front of the two firewalls forwards all incoming traffic to the active firewall. The firewall then applies your policies and forwards the traffic accordingly to the backend VMs. The Azure User Defined Routing Table, which is used for the backend VMs to be able to use the firewall as the default gateway, is updated and monitored by the active firewall after a failover event so that the active firewall is always used as the gateway.

For more information, see High Availability in Azure.

Upload User Images from VHD Files

If you need a specific firmware version of the CloudGen Firewall or Control Center for Azure that is not available in the Marketplace, or you are deploying in a region without access to the Azure Marketplace, download the VHD disk images from the Barracuda Networks download portal, and then upload them to your Azure storage account. Use the uploaded disk images to deploy via Azure PowerShell or Templates.

For more information, see How to Upload Azure VHD Images for User Defined Images using ARM.

Deploy in Azure Germany

If you are deploying to Azure Germany, the Azure Marketplace is not available, limiting your deployment options. Disk images must be uploaded manually and then deployed via Azure PowerShell or Azure Templates. In addition, to use Azure PowerShell, the environment must be added and appended when logging in.

For more information, see Microsoft Azure Deployments in Azure Germany.

Figures

1. azure_arm_single_backend_diagram.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.