Microsoft Azure Deployment

https://campus.barracuda.com/doc/53248673/

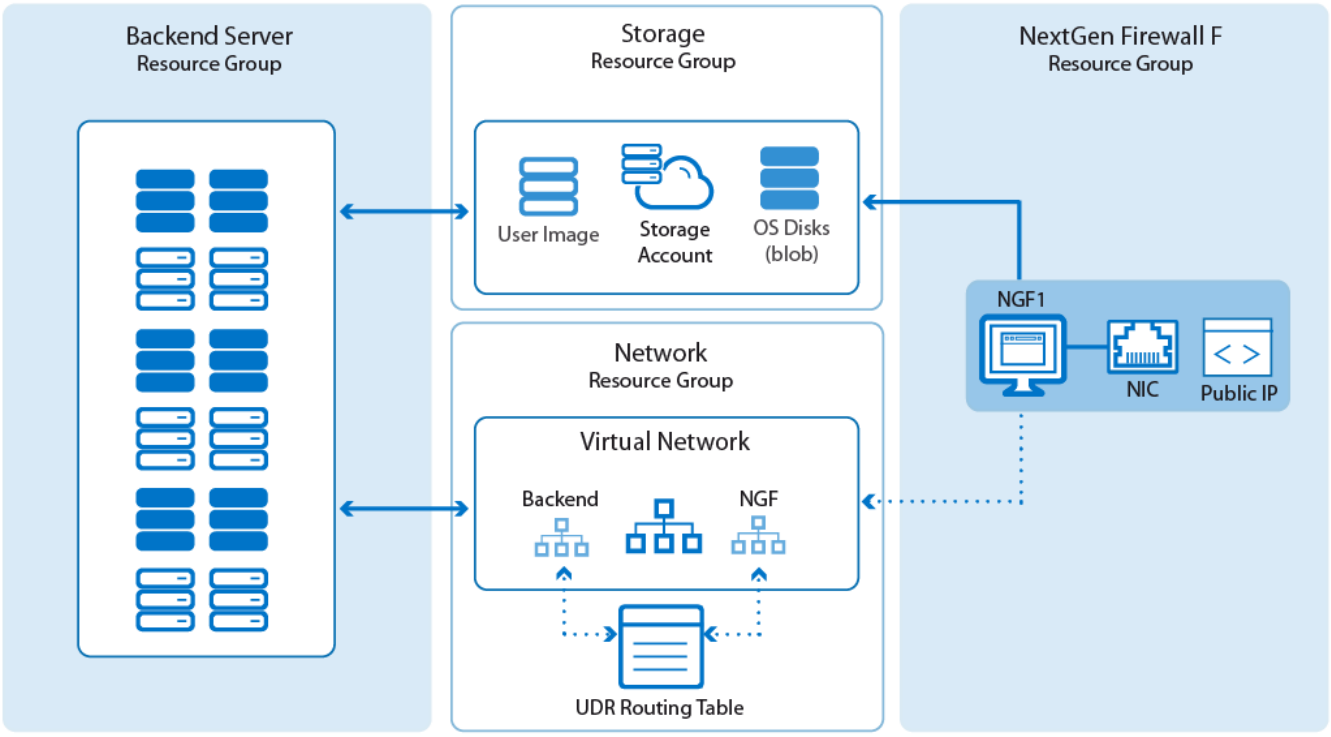
Microsoft Azure offers two ways to deploy and manage your cloud resources:

- **Azure Resource Manager**
- **Azure Service Manager**

Azure Resource Manager (ARM) is the recommended deployment model for new Azure deployments. Grouping your resources into resource groups makes it easy to create setups that are modular. Azure Service Manager (ASM) is the classic model and should no longer be used for new deployments. There are several different configuration and deployment tools available for both ARM and ASM. Not all configuration tools offer the same functionality. New features are usually first available via PowerShell, Azure templates, and REST API, with the web portal catching up later.

	ARM	ASM
Web Portal	Yes - https://portal.azure.com	No
Azure Templates	Yes	No
Azure PowerShell	Yes (version 1.0 or higher)	Yes
REST API	Yes	Yes
Azure CLI	Yes	Yes

Azure Resource Manager



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, access control ,and billing for your applications. Resource groups also make it easier to redeploy 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.

Deploy an F-Series Firewall or Control Center via Azure Portal

The Azure portal allows you to deploy the Barracuda NextGen Firewall F and NextGen Control Center images from the Azure Marketplace using an easy-to-use web interface. The web portal is not always feature-complete compared to the other deployment options.

For more information, see How to Deploy a F-Series Firewall in Microsoft Azure using Azure Portal and ARM.

Deploy an F-Series 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 an F-Series Firewall in Microsoft Azure Using PowerShell and ARM.

Deploy an F-Series Firewall or Secure Access Concentrator via Azure Solution Templates

Azure solution templates allow you to deploy one of the multiple preconfigured solutions depending on your use case in Azure. The following solutions are available in the Azure Marketplace:

- Single, stand-alone F-Series Firewall including Azure Route Table. The firewall is deployed into a dedicated subnet. Both PAYG and BYOL versions are available.
- Single, managed F-Series Firewall including Azure Route Table. The firewall fetches the configuration directly from your Control Center on deployment.
- A single managed NextGen Secure Access Concentrator. The SAC fetches the configuration directly from your Control Center on deployment.

For more information, see Azure Solution Templates for F-Series Firewalls.

Deploy an F-Series 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 Azure PowerShell, Azure CLI, 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 an F-Series Firewall via Azure Templates.

Lab Guide: Getting Started with the Barracuda NextGen Firewall F on Azure

In this lab you will learn how to:

- Deploy a Barracuda NextGen Firewall
- Configure Azure networking the F-Series Firewall
- Set user defined roles, create traffic routing rules, and control the flow of traffic between virtual machines

Download the Lab Guide: Working with the F-Series Firewall in Azure.

Modifying a NextGen Firewall Azure Template to Retrieve the PAR File

If you are using the NextGen Control Center either on-premises or in the cloud, modify the Azure template to retrieve the PAR file for the new F-Series 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 an F-Series 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 F-Series 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 download portal, and then upload them to your Azure storage account. Use the uploaded disk images to deploy via Azure PowerShell or Templates.

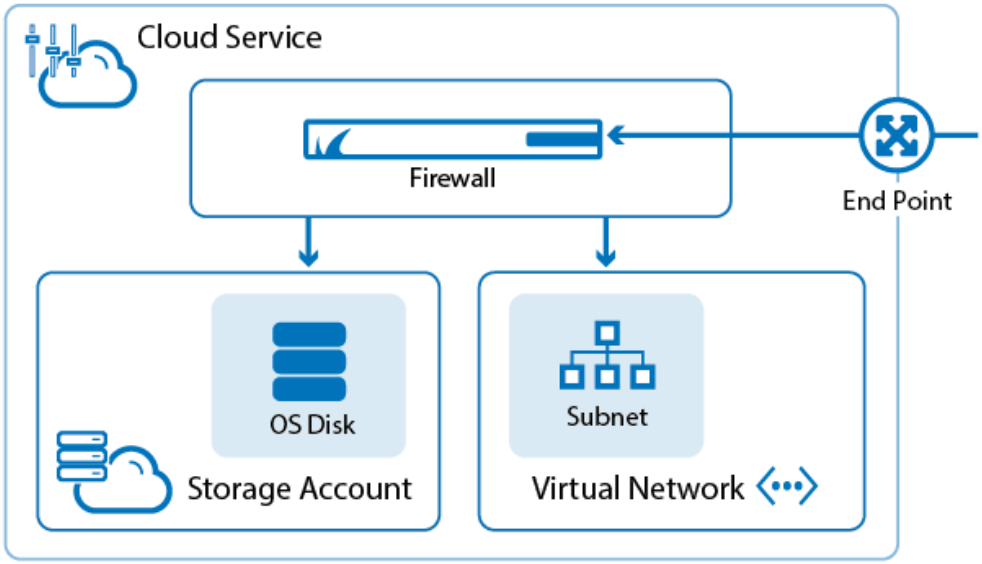
For more information, see How to Upload Azure VHD Images for User Defined Images using ARM.

Deploy in Azure Germany

If you are deploying to the 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.

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

Azure Service Manager



Azure Service Manager is the classic deployment model. ASM organizes your virtual machines into compute containers called cloud services and additionally uses a virtual network containing subnets to segregate your virtual machines according to their purpose. During the transition to the Resource Manager model, classic resources were automatically placed into a resource group. While it is possible to move these resources to other resource groups, Microsoft does not allow you to mix ASM and ARM deployments; instead, it recommends you to redeploy your resources using ARM.

For more information, see Microsoft Azure Deployments using Azure Service Manager (ASM).

Figures

1. azure_arm_single_backend_diagram01.png
2. 06_service_mgmt_concept.png