Microsoft Azure Deployments using Azure Service Manager (ASM)

https://campus.barracuda.com/doc/53248674/

Azure Service Manager (ASM) is the classic deployment mode used in legacy Azure deployments. ASM offers a PowerShell for deployments. The following deployments are available:

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

For most advanced networking features in the Microsoft Azure Cloud, such as multiple network interfaces or reserved IP addresses for the cloud service, you must deploy the Barracuda NextGen Firewall F via PowerShell. Using a custom PowerShell script allows for rapid deployment and fast recovery in case of failure. The NextGen Control Center for Microsoft Azure is deployed just like the F-Series Firewall except that it is limited to one network interface. The number of network interfaces depends on the Instance size.

Fore more information, see How to Deploy the Barracuda F-Series Firewall in Azure via PowerShell and ASM.

Upload and Create Images from VHD Files using ASM

If you are deploying in a region that does not offer access to the Azure Marketplace, or you want to deploy a specific firmware version that is no longer offered in the Marketplace, you can upload F-Series Firewall or NextGen Control Center images. The VHD disk images are available in the Barracuda Download Portal and must uploaded to your Azure storage account. Then, you can create a custom image using the uploaded disk image.

For more information, see How to Create a Barracuda F-Series Firewall Azure Image from a VHD Disk Image using ASM.

Deploy an F-Series Firewall High Availability Cluster using ASM

To avoid downtime when the primary firewall is unavailable due to maintenance or hardware faults, configure a high availability cluster. Load-balanced endpoints forward the matching incoming traffic to the active firewall. The firewall then applies your policies and forwards the traffic to the backend VMs.

For more information, see High Availability in Azure.

Add and Remove Data Disks for Existing Firewalls in Azure

Data disks allow you to utilize the I/O limit and Azure storage architecture better than when using a single OS disk. The data disks are added to a RAID0 and mounted on /phion0/. Data disks can be

added during deployment with Azure templates or PowerShell.

For more information, see How to Add and Remove Data Disks in Azure using ASM.