

---

## Microsoft Azure Deployment

<https://campus.barracuda.com/doc/46895218/>

Microsoft Azure offers two deployment modes: Resource Manager (ARM) and Azure Service Manager (ASM). Azure Resource Manager (ARM) is the recommended deployment mode for new Azure deployments. Grouping your resources into resource groups makes it easy to create setups that are modular and allow you to replace resources by swapping resource groups. ASM is the legacy mode and should no longer be used. Deployment types should not be mixed. Microsoft offers several choices how you can deploy your VMs and Azure resources. Both ASM and ARM offer a web portal and/or PowerShell.

### Azure Resource Manager

---

You can use the Azure web portal as well as Azure PowerShell for your deployments. Some advanced features are not yet available in the web portal and require Azure PowerShell to deploy.

#### 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. Due to the limited features of the portal, you cannot deploy via the web interface if you need to use storage, network resources in different resource groups, UDR, or user images.

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 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, you can download the VHD disk images from the Barracuda download portal, and then upload them to your Azure storage account. You can then use these user images to deploy via Azure PowerShell or Template.

For more information, see [How to Upload Azure VHD Images for User Defined Images using ARM](#).

## **Azure Service Manager**

---

Azure Service Manager (ASM) is the classic deployment mode. You can also deploy using Azure Service Manager using PowerShell or the Azure CLI.

For more information, see [Microsoft Azure Deployments using Azure Service Manager \(ASM\)](#).

© Barracuda Networks Inc., 2021 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.