Cloud Deployment Guide (Azure)

FortiProxy 7.0

January 12, 2024
FortiProxy 7.0 Cloud Deployment Guide (Azure)
45-700-674631-20240112

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-04-01	Initial release.
2023-10-19	Major updates with more details about FortiProxy VM deployment on Azure.
2023-12-01	Updated the following topics: • Deploying FortiProxy-VM from a VHD image file on page 11 • Deploying FortiProxy-VM from the Azure marketplace on page 8
2024-01-12	Updated Models on page 6.

Overview

FortiProxy is available for deployment on Microsoft Azure, which is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through a global network of Microsoft-managed data centers. FortiProxy for Azure supports single VM deployment and active/passive high availability (HA) configuration. HA enables configuration synchronization and failover management between the primary and secondary FortiProxy instances. When the FortiProxy detects a failure, the passive FortiProxy instance becomes active.

Azure services and components

FortiProxy-VM for Azure is a Linux VM instance. The following table lists Azure services and components required to be understood when deploying FortiProxy-VM. All services and components listed relate to ordinary FortiProxy-VM single instance deployment or FortiProxy-native active-passive HA deployment.

Service/component	Description
Azure Virtual Network (VNet)	This is where the FortiProxy-VM and protected VMs are situated and users control the network. When you deploy Proxy-VM, you can configure relevant network settings.
VM	FortiProxy-VM for Azure is a customized Linux VM instance.
Subnets, route tables	You must appropriately configure the FortiProxy-VM with subnets and route tables to handle traffic. When deploying from the marketplace launcher, there are two subnets for the FortiProxy-VM labeled `PublicFacingSubnet` and `InsideSubnet` by default.
Resource group	A group of resources where the FortiProxy-VM is deployed.
Availability Set	An availability set is a logical grouping capability that you can use in Azure to ensure that the VM resources you place within it are isolated from each other when they are deployed within an Azure datacenter. Usually a set intends to accommodate multiple VMs.
Public DNS IP address	You must allocate at least one public IP address to the FortiProxy-VM to access and manage it over the Internet.
Security groups	Unlike AWS, you cannot configure Azure security groups at the time of FortiProxy-VM deployment. All traffic is allowed inbound to, or outbound from, the subnet, or network interface by default. See Default security rules.
VHD	A special type of deployable image used for Azure. As long as you deploy FortiProxy-VM from the marketplace launcher, you do not need VHD files. However, you can launch FortiProxy-VM (BYOL) directly from the FortiProxy-VM VHD image file instead of using the marketplace. Ask azuresales@fortinet.com to find out where you can obtain the VHD images if needed.
Load Balancer	A network LB automatically distributes traffic across multiple FortiProxy-VM instances when configured properly. Topologies differ depending on how you distribute incoming and outgoing traffic.

Instance type support

You can deploy FortiProxy-VM as bring your own license (BYOL) on Azure on all available instances that the FortiProxy-VM supports. Supported instances on Azure for new deployments may change without notice.

Models

FortiProxy-VM is available with different CPU sizes. You can deploy FortiProxy-VM on various private and public cloud platforms. The following table shows the models conventionally available to order, also known as bring your own license (BYOL) models. See Licensing on page 6.

Model name	vCPU	
	Minimum	Maximum
VM02	1	4
VM04	1	8
VM08	1	16
VM16	1	32
VMUL	1	Unlimited

For information about each model's order information, capacity limits, and adding VDOM, see the FortiProxy datasheet.

Licensing

You must have a license to deploy FortiProxy for Azure. On Azure, there is one order type for FortiProxy: bring-your-own-license (BYOL), which offers perpetual (normal series and v-series) and annual subscription (s-series) licensing. Subscription is month-based. BYOL licenses are available for purchase from resellers or your distributors, and the publicly available price list, which Fortinet updates quarterly, lists prices. BYOL licensing provides the same ordering practice across all private and public clouds, no matter what the platform is. You must activate a license for the first time you access the instance from the GUI or CLI before you can start using various features.

For BYOL, cloud vendors charge separately for resource consumption on computing instances, storage, and so on, without use of software running on top of it (in this case the FortiProxy-VM). You typically order a combination of products and services including support entitlement.

To proceed with licensing a BYOL deployment and make use of Fortinet technical support, you must obtain a license, register it in FortiCloud, and activate the FortiProxy-VM:

1. Obtain licenses for the BYOL licensing model through any Fortinet partner. If you do not have a partner, contact jerrywang@fortinet.com for assistance in purchasing a license. You will receive a PDF with an activation code.
2. If you do not have a FortiCloud account, create one here by following the instructions in the FortiCloud documentation.

3. Register your license in your FortiCloud account by following the instructions in the FortiCloud documentation. Doing so allows our support team to identify your registration in the system.
4. Download the license (`.lic`) file to your computer as you will be prompted to upload this license to activate the FortiProxy-VM during the first login. Activation is required before you can configure the FortiProxy-VM.

It may take up to 30 minutes for Fortinet servers to fully recognize the new license. If you get an error that the license is invalid when uploading the license (`.lic`) file to activate the FortiProxy-VM, wait 30 minutes and try again.

Deploying FortiProxy-VM from the Azure marketplace

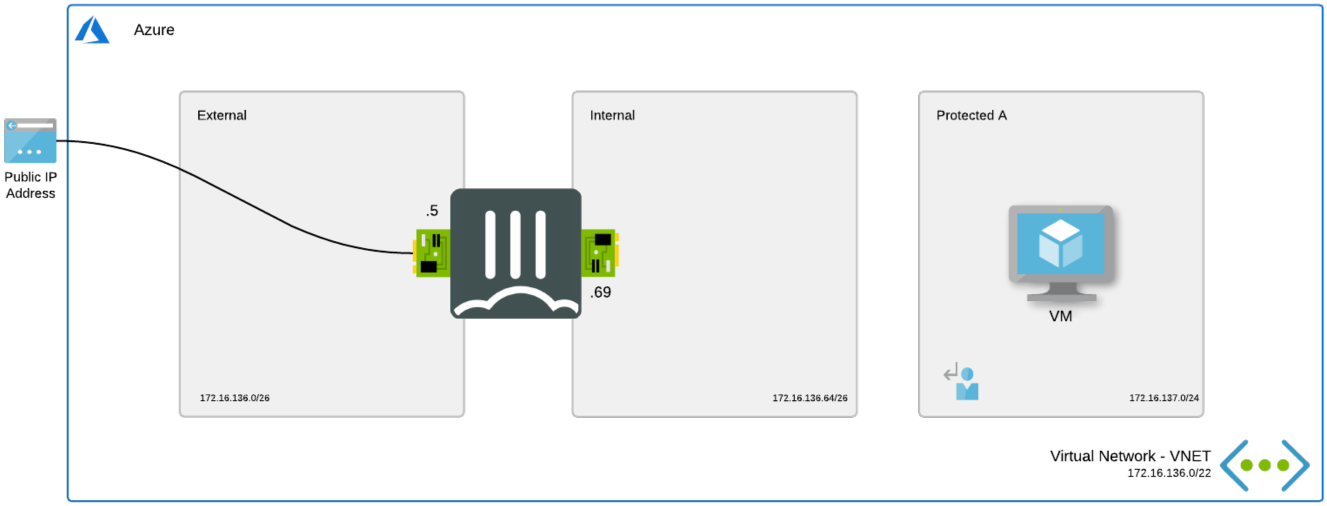
You can deploy FortiProxy-VM as a virtual appliance in the Azure cloud (infrastructure as a service (IaaS)) from the Azure marketplace. This section shows you how to install and configure a single instance FortiProxy-VM in Azure to provide a secure web gateway solution in front of Azure IaaS resources.

> You can only deploy certain versions of the FortiProxy 7.0 VM from the Azure marketplace. To install other versions or a custom image, see Deploying FortiProxy-VM from a VHD image file on page 11.

This section covers the deployment of simple web servers, but you can use this deployment type for any type of public resource protection with only slight modifications. With this architecture as a starting point, you can implement more advanced solutions, including multi-tiered solutions.

The example in this document creates three subnets:

Subnet	Description
Subnet1	External subnet used to connect the FortiProxy-VM to the Internet.
Subnet2	Internal subnet used as a transit network to one or multiple protected networks containing backend services, such as the web server.
Subnet3	Protected subnet used to deploy services. You can deploy multiples of these subnets. The traffic is sent to the FortiProxy for inspection using UDR.



To deploy the FortiProxy-VM from the Azure marketplace:

1. In the Azure dashboard, select *Create a resource*.
2. Search for *FortiProxy* to locate the *Fortinet FortiProxy Secure Web Gateway (SWG)* listing.
3. Open the listing and click *Get It Now*.
4. Click *Continue*, select *FortiProxy Single VM*, and click *Create*.

5. Configure the options on the *Basics* tab according to your requirements:
   a. For *Resource Group*, create a new resource group or select an existing one. Deploying the solution to a new or empty resource group is recommended. You can deploy the solution to an existing resource group that already contains resources, but this may overwrite existing resources.
   b. From the *Region* dropdown list, select the desired region. FortiProxy-VM is available in all public regions of Azure and the China and Gov regions. Availability depends on the access rights of the Azure subscription used for deployment.
   c. In the *FortiProxy administrative username* and *password* fields, enter the username and password for the FortiProxy administrative profile.
   d. In the *FortiProxy Name Prefix* field, assign a naming prefix for your FortiProxy resources.
   e. From the *FortiProxy Image SKU* dropdown list, select *Bring Your Own License*.
   f. From the *FortiProxy Image Version* dropdown list, select the FortiProxy version to deploy. To install versions that are not available in the list or to install a custom image, see Deploying FortiProxy-VM from a VHD image file on page 11.
   g. Click *Next*.
6. On the *Instance* tab, select an availability option, upload your FortiProxy license (see Licensing on page 6), specify the name of the FortiProxy VM, and click *Next*.
7. On the *Networking* tab, configure the networks:
   a. Create a new virtual network to deploy the FortiProxy.
   b. Create three subnets as the FortiProxy-VM requires a public and private interface for Internet edge protection.
   c. Enable or disable *Accelerated Networking*, which refers to SR-IOV support. This depends on the instance type that you selected.
   d. Click *Next*.
8. On the *Public IP* tab, create a new public IP address or create a new one. Click *Next*.
9. On the *Advanced* tab, configure the parameters according to your requirements:
   a. To allow FortiManager to manage this FortiProxy, enable *Connect to FortiManager* and provide the FortiManager IP address and serial number in the *FortiManager IP address* and *FortiManager Serial Number* fields.
   b. In the *Custom Data* field, add initial configuration for the FortiProxy deployment if desired. For example, you can enter FortiProxy CLI commands which will then be executed during the initial bootup of the FortiProxy.
   c. Enable or disable serial console as needed using the *Enable Serial Console* field.
   d. Leave the *Custom VHD* field empty. This field is used only if you are deploying the FortiProxy VM from a custom VHD file. See Deploying FortiProxy-VM from a VHD image file on page 11.
   e. Click *Review + create*.
10. When validation passes, click *OK*.

If you want to download the template, click *Download template and parameters*.

11. Click *Create*. You should see the deployment progress and the parameters and template that Azure is processing. Once deployed, the new resources show in the resource group.
12. Connect to the FortiProxy-VM by following the steps below:
    a. Open the FortiProxy Public IP resource and copy the IP address that Azure assigned.
    b. In a web browser, connect to the IP address using HTTPS on port 443. You can also use an SSH client on port 22.
    c. The system displays a warning that the certificate is untrusted. This is expected since the FortiProxy-VM is using a self-signed certificate. If desired, replace the certificate with a signed certificate.

d. Sign in with the credentials specified in the Azure template parameters.
e. If you did not upload a license during the deployment, upload the license now and reboot the FortiProxy-VM before continuing. See Licensing on page 6.

Deploying FortiProxy-VM from a VHD image file

You can deploy a FortiProxy-VM (BYOL) using a VHD file of any desired version or build that is outside the marketplace product listing in the Azure portal.

Obtain the FortiProxy VHD image file

1. Go to https://support.fortinet.com.
2. Click *Login* and log in to the Fortinet Support website.
3. From the *Support > Downloads* menu, select *Firmware Download*.
4. In the *Select Product* dropdown menu, select *FortiProxy*.
5. On the *Download* tab, navigate to the FortiProxy Azure firmware file in the *Image Folders/Files* section. For example: `FPX_AZURE-v100-buildXXXX-FORTINET.out.hyperv.zip`, Where `XXXX` is the build number.
6. Click *HTTPS* to download the firmware.
7. Unzip it and locate the `fortios.vhd` file.
8. Upload the `fortios.vhd` file to the `blob/storage` location.

Create an Azure image definition

You can create an image definition via the Azure portal or CLI. See Store and share images in an Azure Compute Gallery and Create a gallery for storing and sharing resources. The following summarizes recommended parameter values to set for the image definition:

Parameter	Recommended value
`subscription ID`	Enter the subscription ID if the tenant has multiple subscriptions.
`publisher`	`Fortinet`
`os-type`	`linux`
`architecture`	`Arm64`
`hyper-v-generation`	`V2`
`os-state`	`Generalized`

You can configure other parameters as fits your requirements. See az sig image-definition create. Under the newly created VM definition, you can create a new image version.

To create an image version:

1. In the Azure portal, go to the VM image definition.
2. Click *Add Version*.
3. Enter the subscription and resource group information.
4. Under *Version details*, configure the following:
   a. For *Version Number*, enter the image version number.
   b. For *Source*, select *Storage blobs (VHDs)*.

  c. For *Os Disk*, browse to the VHD that you uploaded to the storage account earlier.

After Azure creates the image version, you can deploy a new FortiProxy-VM from the image.

Deploy the FortiProxy-VM from the Azure VHD image

1. In the Azure dashboard, select *Create a resource*.
2. Search for *FortiProxy* to locate the *Fortinet FortiProxy Secure Web Gateway (SWG)* listing.
3. Open the listing and click *Get It Now*.
4. Click *Continue*, select *FortiProxy Single VM*, and click *Create*.
5. Configure the options on the *Basics* tab according to your requirements:
   a. For *Resource Group*, create a new resource group or select an existing one. Deploying the solution to a new or empty resource group is recommended. You can deploy the solution to an existing resource group that already contains resources, but this may overwrite existing resources.
   b. From the *Region* dropdown list, select the desired region. FortiProxy-VM is available in all public regions of Azure and the China and Gov regions. Availability depends on the access rights of the Azure subscription used for deployment.
   c. In the *FortiProxy administrative username* and *password* fields, enter the username and password for the FortiProxy administrative profile.
   d. In the *FortiProxy Name Prefix* field, assign a naming prefix for your FortiProxy resources.
   e. From the *FortiProxy Image SKU* dropdown list, select *Bring Your Own License*.
   f. Leave the *FortiProxy Image Version* option as it is. To install versions that are available in the list, see Deploying FortiProxy-VM from the Azure marketplace on page 8.
   g. Click *Next*.
6. On the *Instance* tab, select an availability option, upload your FortiProxy license (see Licensing on page 6), specify the name of the FortiProxy VM, and click *Next*.
7. On the *Networking* tab, configure the networks:
   a. Create a new virtual network to deploy the FortiProxy.
   b. Create three subnets as the FortiProxy-VM requires a public and private interface for Internet edge protection.
   c. Enable or disable *Accelerated Networking*, which refers to SR-IOV support. This depends on the instance type that you selected.
   d. Click *Next*.
8. On the *Public IP* tab, create a new public IP address or create a new one. Click *Next*.
9. On the *Advanced* tab, configure the parameters according to your requirements:
   a. To allow FortiManager to manage this FortiProxy, enable *Connect to FortiManager* and provide the FortiManager IP address and serial number in the *FortiManager IP address* and *FortiManager Serial Number* fields.
   b. In the *Custom Data* field, add initial configuration for the FortiProxy deployment if desired. For example, you can enter FortiProxy CLI commands which will then be executed during the initial bootup of the FortiProxy.
   c. Enable or disable serial console as needed using the *Enable Serial Console* field.
   d. In the *Custom VHD* field, upload the custom FortiProxy image that you created earlier by entering the resource ID of the image.
   e. Click *Review + create*.

10. When validation passes, click *OK*.

If you want to download the template, click *Download template and parameters*.

11. Click *Create*. You should see the deployment progress and the parameters and template that Azure is processing. Once deployed, the new resources show in the resource group.
12. Connect to the FortiProxy-VM by following the steps below:
    a. Open the FortiProxy Public IP resource and copy the IP address that Azure assigned.
    b. In a web browser, connect to the IP address using HTTPS on port 443. You can also use an SSH client on port 22.
    c. The system displays a warning that the certificate is untrusted. This is expected since the FortiProxy-VM is using a self-signed certificate. If desired, replace the certificate with a signed certificate.
    d. Sign in with the credentials specified in the Azure template parameters.
    e. If you did not upload a license during the deployment, upload the license now and reboot the FortiProxy-VM before continuing. See Licensing on page 6.

HA for FortiProxy-VM on Azure

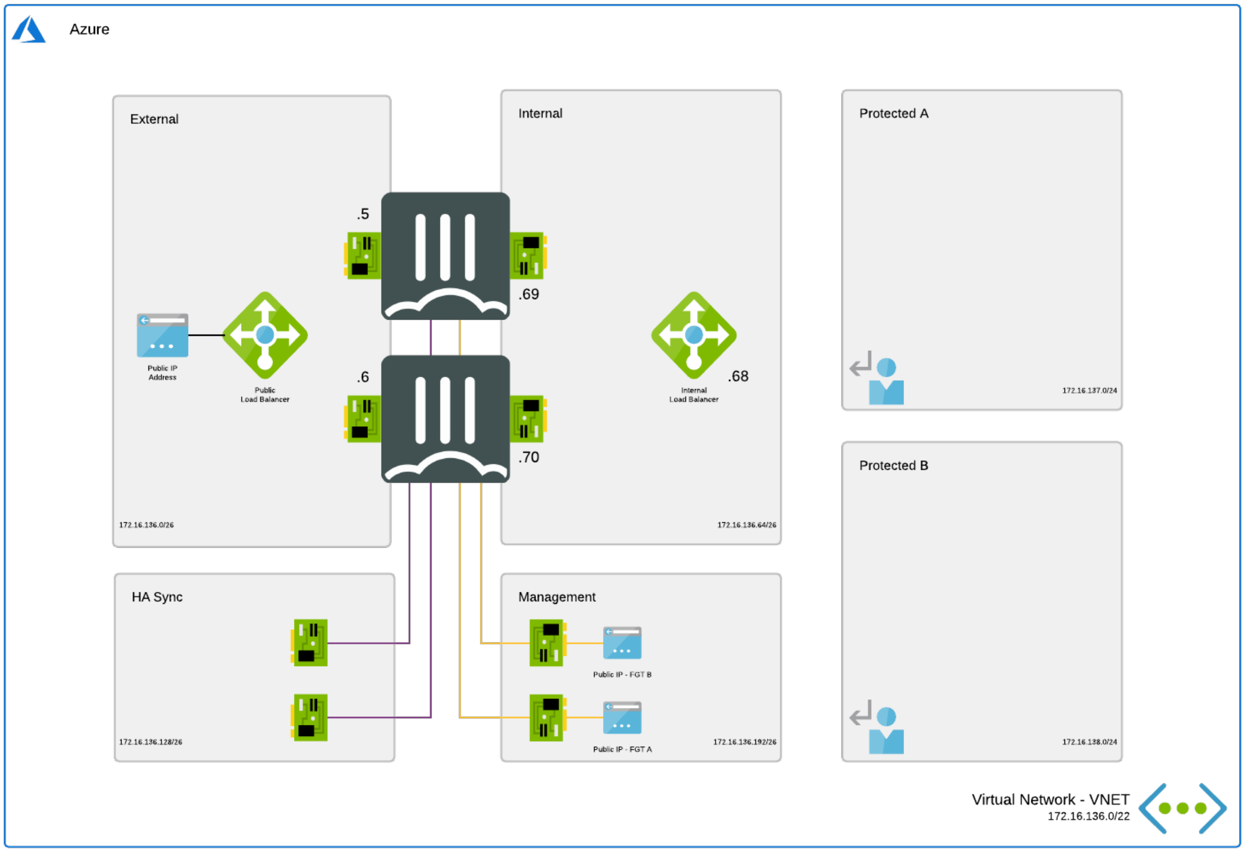
When designing a reliable architecture in Azure, you must take resiliency and high availability (HA) into account. See Microsoft's Overview of the reliability pillar. Running FortiProxy inside Azure offers different reliability levels depending on the building blocks used.

Microsoft offers different SLAs on Azure based on the deployment that you use:

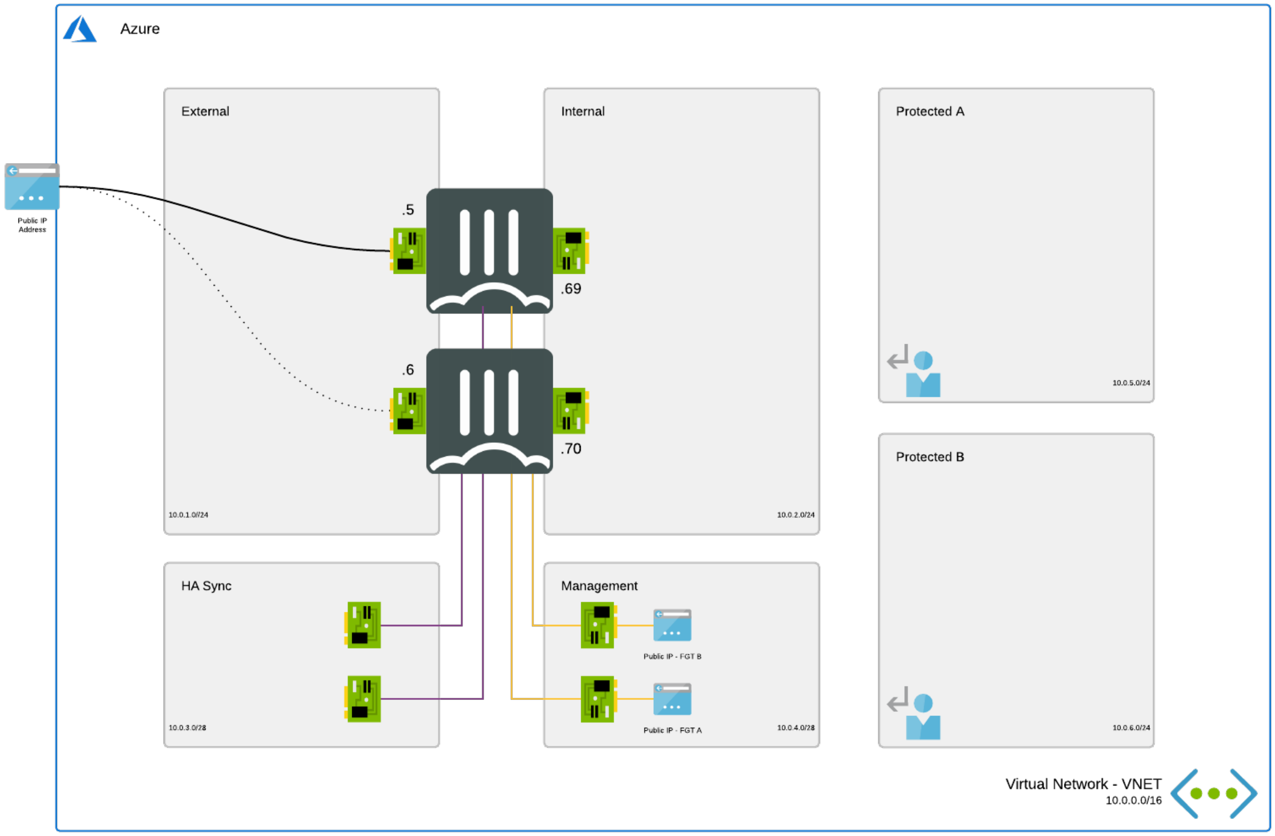
- Availability Zone (AZ) (different datacenter in the same region): 99.99%
- Availability Set (different rack and power): 99.95%
- Single VM with premium SSD: 99.9%

Building blocks

- **Active-passive with external and internal Azure load balancer (LB):** this design deploys two FortiProxy-VMs in active-passive mode connected using unicast FortiProxy clustering protocol (FGCP) HA protocol. In this setup, the Azure LB handles traffic failover using a health probe towards the FortiProxy-VMs. The failover times are based on the health probe of the Azure LB: 2 failed attempts per 5 seconds with a maximum of 15 seconds. You configure the public IP addresses on the Azure LB. The public IP addresses provide ingress and egress flows with inspection from the FortiProxy. Microsoft provides guidance on this architecture.



- **Active-passive HA with SDN connector failover**: This design deploys two FortiProxy-VMs in active-passive mode connected using the unicast FGCP HA protocol. This protocol synchronizes the configuration. On failover, the passive FortiProxy takes control and issues API calls to Azure to shift the public IP address and update the internal user-defined routing to itself. Shifting the public IP address and gateway IP addresses of the routes takes time for Azure to complete. Microsoft provides a general architecture. In FortiProxy's case, the API calls logic is built-in instead of requiring additional outside logic like Azure Functions or ZooKeeper nodes.



Availability zones and availability sets are available as options in the Azure marketplace. You can select them during deployment.

Deploying FortiProxy HA using Terraform

Use the Terraform code in the GitHub page to deploy FortiProxy Active-passive HA across two availability zones. Refer to the README.md file on the page for detailed deployment instructions.

Visit the FortiProxy Terraform Azure GitHub project page for a complete list of FortiProxy Azure solutions. For issues, see this GitHub project's Issues tab. For other questions related to the GitHub project, contact github@fortinet.com.

www.fortinet.com