www.ibs.com.cy

CONFIGURING FORTIGATE AZURE VIRTUAL MACHINE

By Marios Tsimaris - Senior Systems Engineer

INTRODUCTION

By combining stateful examination with a comprehensive suite of heavy-duty security features, the FortiGate- Virtual Machine delivers next-generation firewall (NGFW) capabilities for organizations of all sizes, with the inflexibility to be stationed as NGFW and/ or VPN gateway. It protects against cyber dangers with high performance, security efficacity, and deep visibility. This answer is available for deployment on Microsoft Azure, and in this composition, we will cover several ways how you can configure your Virtual FortiGate, but the easiest and most common way is the download it from the marketplace when you log in to Microsoft Azure.

FORTIGATE-VM FROM A VHD IMAGE FILE

You can deploy FortiGate using custom templates from VHD image files. These files you'll find these from Fortinet Customer Service and Support. Once you've got downloaded your Fortinet product from there, you unzip the file and locate the fortios.vhd file. Upload this file to your storage location as required by your deployment template.

FORTIGATE-VM WITH A CUSTOM ARM TEMPLATE

Using a customized ARM template in the Azure Portal, you may deploy a FortiGate-VM and bring your license (BYOL) outside the corporate product catalog. If you wish to install FortiGate- VM on case kinds and sizes that the FortiGate- VM marketplace launcher does not support, you must use this system. Due to a lack of certified FortiGate- VM prototype support, some of the prototype kinds of your choice might not properly start up or run. For your deployment, a bare minimum collection of templates is offered. Additionally, you may include bootstrapping FortiGate CLI commands in the template and run them during the first bootup.

FORTIGATE-VM USING AZURE POWERSHELL

Using Azure PowerShell, you may configure FortiGate-VM (BYOL) outside of the marketplace product catalog. If you wish to install FortiGate-VM on example type sizes that aren't configured on the FortiGate marketplace launcher, this is an alternative method. Due to a lack of authorized FortiGate instance support, some of the sample types of your choice might not properly boot up or execute. Additionally, you may define the bootstrapping FortiGate CLI commands in a configuration file that is sent to PowerShell during the first bootup. To use this deployment strategy, it is expected that you have an in-depth understanding of PowerShell and numerous Azure services and functionalities.

FORTIGATE-VM ON REGIONAL AZURE CLOUDS

Along with "global" Azure support, FortiGate-VM also offers "regional" Azure support for countries like China, Germany, and the US government. Because they are not covered by global Azure and because the services are run under URL domains exclusive to the regional Azure cloud, FortiGate-VM deployment on regional Azure clouds requires devoted subscription accounts. There are no regional Azure cloud marketplaces that provide FortiGate-VM. Instead, you may install FortiGate-VM (BYOL) by preparing a VHD file and customizing a FortiGate-VM instance using your PowerShell or ARM deployment templates by referring to the VHD file.

FORTIGATE-VM FROM THE MARKETPLACE

1. Search for and select Fortinet FortiGate Next-Generation Firewall in the Azure marketplace.
2. Select the desired deployment plan from the Select a Plan and click Create.
3. Configure the parameters according to your requirements on the Basics tab:
   a) Select your subscription from the Subscription dropdown list
   b) Select an existing resource group or create a new one in Resource group
   c) Select the desired region from the Region dropdown list
   d) Enter the username and password for the FortiGate administrative profile in the FortiGate administrative username and password fields
   e) Assign a naming prefix for your FortiGate resources in the FortiGate Name Prefix field
   f) Select BYOL or PAYG from the FortiGate Image SKU dropdown list
   g) Select the FortiGate version to deploy from the FortiGate Image Version dropdown list
   h) Click Next
4. Select an appropriately sized instance type on the Instance Type tab, and then click Next
5. Configure the parameters according to your requirements on the Networking tab:
   a) Select an existing VNet or create a new one in Virtual network. A public and private interface for Internet edge protection is required for FortiGate-VM.
   b) Enable or disable Accelerated Networking, which refers to SR-IOV support and depends on the instance type you selected.
   c) Click Next
6. Create a new public IP address or create a new one on the Public IP tab, and then click Next
7. Configure the parameters according to your requirements on the Advanced tab:

   a) You may enable Connect to Forti Manager and provide the Forti Manager IP address and serial number in the Forti Manager IP address and Forti Manager Serial Number fields if you want Forti Manager to manage this FortiGate
   b) You may enter the desired commands in the Custom Data field if you want to provide initial configuration to the FortiGate. These commands are executed during the first bootup.
   c) Use the FortiGate License field to submit a BYOL license file for the FortiGate. If you chose PAYG in step 3, the license file is not taken into account. Click Next

8. Confirm all values once validation completes, and then click Create. The resources are created appropriately by Azure.

IBSCY Ltd is a certified silver partner of Fortinet in Cyprus which is one of the leading global companies in cybersecurity solutions. We are authorized to sell, configure, maintain, and support all Fortigate devices in Cyprus. As a certified IT company, we guarantee fast and professional IT solutions for any kind and size of business.

	Marios Tsimaris is a Senior Systems Engineer of IBSCY for the last 3 years. He is a member of the IT department which consists of 5 people, and it is responsible for the day-to-day support and maintenance of our clients as well as for the implementations of new and existing clients. He holds several certifications from Microsoft, Fortinet, VMWare and other vendors.