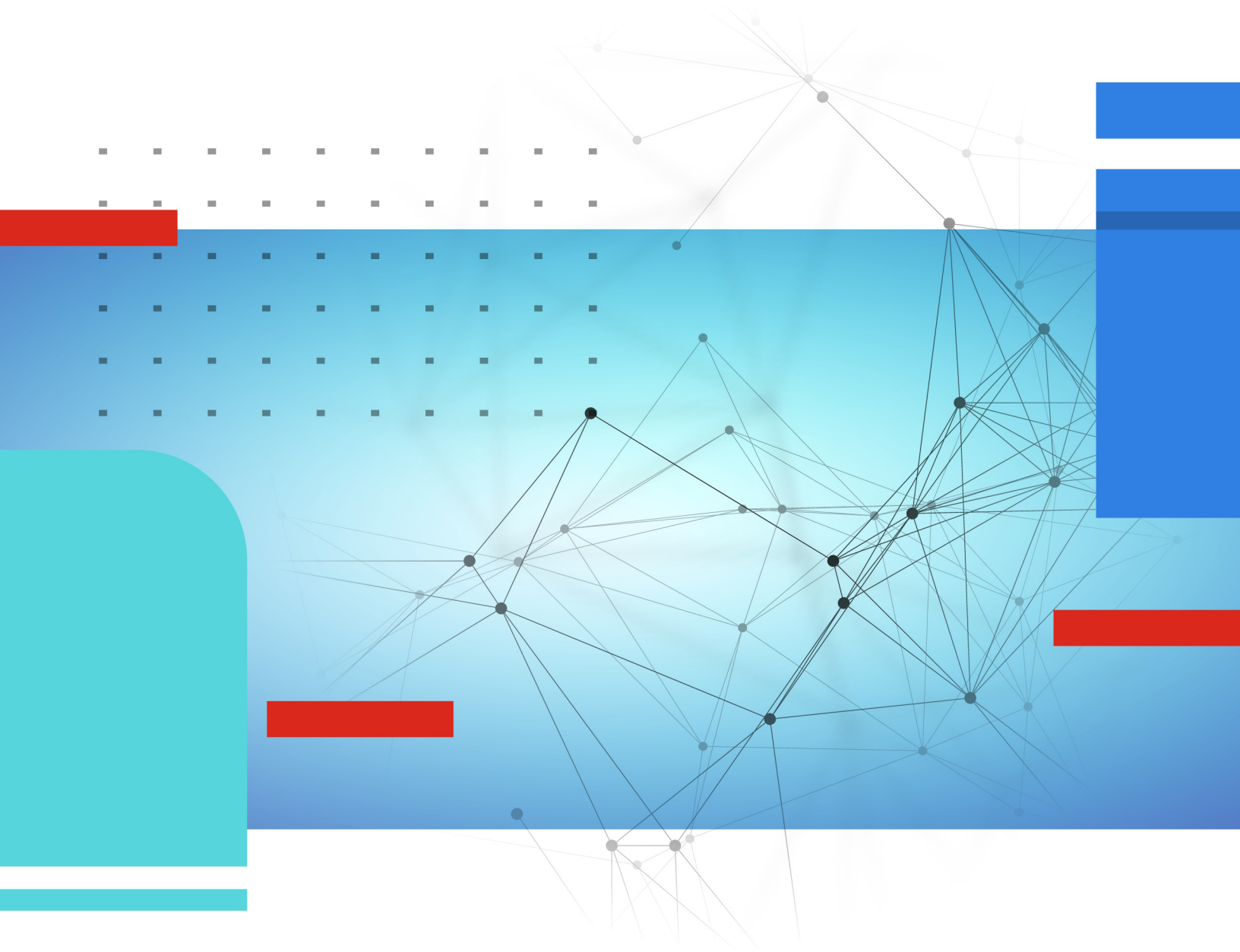
Azure Administration Guide

FortiOS 7.6



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

November 28, 2024
FortiOS 7.6 Azure Administration Guide
01-76-1054269-20241128

TABLE OF CONTENTS

About FortiGate-VM for Azure

By combining stateful inspection with a comprehensive suite of powerful security features, FortiGate next generation firewall technology delivers complete content and network protection. This solution is available for deployment on Microsoft Azure.

In addition to advanced features such as an extreme threat database, vulnerability management, and flow-based inspection, features including application control, firewall, antivirus, IPS, web filter, and VPN work in concert to identify and mitigate the latest complex security threats.

FortiGate-VM for Azure supports active/passive high availability (HA) configuration with FortiGate-native unicast HA synchronization between the primary and secondary nodes. When the FortiGate-VM detects a failure, the passive firewall instance becomes active and uses Azure API calls to configure its interfaces/ports.

FortiGate-VM also supports active/active HA using Azure load balancer.

Highlights of FortiGate-VM for Azure include the following:

- Delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features.
- IPS technology protects against current and emerging network-level threats. In addition to signature-based threat detection, IPS performs anomaly-based detection, which alerts users to any traffic that matches attack behavior profiles.
- Docker application control signatures protect your container environments from newly emerged security threats. See FortiGate-VM on a Docker environment.

FortiOS 7.6 supports backing up FortiGate Azure VMs using Azure's enhanced backup policy. See the Microsoft documentation.

Instance type support

FortiGate supports the following instance types on Azure.

Supported instances on the Azure marketplace listing may change without notice and may vary between bring your own license (BYOL) and pay as you go. Instance types of the A- and D-series do not appear as deployable instances at the time you install the FortiGate virtual machine (VM) on the marketplace launcher.

For up-to-date information on each instance type, see the following links:

- Sizes for virtual machines in Azure
- Compute optimized virtual machine sizes
- General purpose virtual machine sizes

FortiOS supports hot-adding vCPU and RAM. However, Azure may not support this. See Change the size of a virtual machine.

Having at least 4 GB of RAM for proper FortiGate-VM operation is recommended, especially if UTM is enabled.

Compute-optimized instance types

The following table provides information on compute-optimized instance types:

Instance type	vCPU	Max NIC	Recommended BYOL license
F-series			
Standard_F2	2	2	FG-VM02 or FG-VM02v
Standard_F4	4	4	FG-VM04 or FG-VM04v
Standard_F8	8	8	FG-VM08 or FG-VM08v
Standard_F16	16	8	FG-VM16 or FG-VM16v
Fs-series			
Standard_F2s	2	2	FG-VM02 or FG-VM02v
Standard_F4s	4	4	FG-VM04 or FG-VM04v
Standard_F8s	8	8	FG-VM08 or FG-VM08v
Standard_F16s	16	8	FG-VM16 or FG-VM16v
Fsv2-series			
Standard_F2s_v2	2	2	FG-VM02 or FG-VM02v
Standard_F4s_v2	4	2	FG-VM04 or FG-VM04v
Standard_F8s_v2	8	4	FG-VM08 or FG-VM08v
Standard_F16s_v2	16	4	FG-VM16 or FG-VM16v
Standard_F32s_v2	32	8	FG-VM32 or FG-VM32v

General purpose instance types

The following table provides information on general purpose instance types:

DSv2 and Dsv3-series

Instance type	vCPU	Max NIC	Recommended BYOL license
DSv2-series			
Standard_DS1_v2	1	2	FG-VM01 or FG-VM01v
Standard_DS2_v2	2	2	FG-VM02 or FG-VM02v
Standard_DS3_v2	4	4	FG-VM04 or FG-VM04v

Instance type	vCPU	Max NIC	Recommended BYOL license
Standard_DS4_v2	8	8	FG-VM08 or FG-VM08v
Standard_DS5_v2	16	8	FG-VM16 or FG-VM16v
Dsv3-series			
Standard_D2s_v3	2	2	FG-VM02 or FG-VM02v
Standard_D4s_v3	4	2	FG-VM04 or FG-VM04v
Standard_D8s_v3	8	4	FG-VM08 or FG-VM08v
Standard_D16s_v3	16	8	FG-VM16 or FG-VM16v
Standard_D32s_v3	32	8	FG-VM32 or FG-VM32v

DV4 and DsV4-series

The DV4 and DsV4-series contain support for Intel Xeon (Ice Lake [2020] and Cascade Lake [2018]) for general purpose workloads. The DsV4 series has the option for premium storage. FortiOS 7.4.2 and later versions support this series:

Instance Type	vCPU	Max NIC	Recommended BYOL license
DV4 series			
Standard_D2_v4	2	2	FG-VM02 or FG-VM02v
Standard_D4_v4	4	2	FG-VM04 or FG-VM04v
Standard_D8_v4	8	4	FG-VM08 or FG-VM08v
Standard_D16_v4	16	8	FG-VM16 or FG-VM16v
Standard_D32_v4	32	8	FG-VM32 or FG-VM32v
DsV4 series			
Standard_D2s_v4	2	2	FG-VM02 or FG-VM02v
Standard_D4s_v4	4	2	FG-VM04 or FG-VM04v
Standard_D8s_v4	8	4	FG-VM08 or FG-VM08v
Standard_D16s_v4	16	8	FG-VM16 or FG-VM16v
Standard_D32s_v4	32	8	FG-VM32 or FG-VM32v

Dav4 and Dasv4-series

The Dav4 and Dasv4-series contain support for second generation AMD EPYC 7452 (Rome 2019) for production/multithreaded workloads. The DaSV4 series has the option for premium storage. FortiOS 7.4.2 and later versions support this series:

Instance Type	vCPU	Max NIC	Recommended BYOL license
DaV4 series			
Standard_D2a_v4	2	2	FG-VM02 or FG-VM02v
Standard_D4a_v4	4	2	FG-VM04 or FG-VM04v
Standard_D8a_v4	8	4	FG-VM08 or FG-VM08v
Standard_D16a_v4	16	8	FG-VM16 or FG-VM16v
Standard_D32a_v4	32	8	FG-VM32 or FG-VM32v
DasV4 series			
Standard_D2as_v4	2	2	FG-VM02 or FG-VM02v
Standard_D4as_v4	4	2	FG-VM04 or FG-VM04v
Standard_D8as_v4	8	4	FG-VM08 or FG-VM08v
Standard_D16as_v4	16	8	FG-VM16 or FG-VM16v
Standard_D32as_v4	32	8	FG-VM32 or FG-VM32v

Dv5 and Dsv5-series

The Dv5 and Dsv5-series contain support exclusively for Intel Xeon (Ice Lake [2020]) for general purpose workloads. A premium storage tier is available on Dsv5. FortiOS 7.4.2 and later versions support this series:

Instance Type	vCPU	Max NIC	Recommended BYOL license
DV5 series			
Standard_D2_v5	2	2	FG-VM02 or FG-VM02v
Standard_D4_v5	4	2	FG-VM04 or FG-VM04v
Standard_D8_v5	8	4	FG-VM08 or FG-VM08v
Standard_D16_v5	16	8	FG-VM16 or FG-VM16v
Standard_D32_v5	32	8	FG-VM32 or FG-VM32v
DsV5 Series			
Standard_D2s_v5	2	2	FG-VM02 or FG-VM02v
Standard_D4s_v5	4	2	FG-VM04 or FG-VM04v
Standard_D8s_v5	8	4	FG-VM08 or FG-VM08v
Standard_D16s_v5	16	8	FG-VM16 or FG-VM16v
Standard_D32s_v5	32	8	FG-VM32 or FG-VM32v

Dasv5 and Dadsv5-series

The Dasv5 and Dadsv5-series contain support for third generation AMD EPYC 7763v (Milan 2021) for production/multithreaded workloads. FortiOS 7.4.2 and later versions support this series:

Instance Type	vCPU	Max NIC	Recommended BYOL license
DasV5 Series			
Standard_D2as_v5	2	2	FG-VM02 or FG-VM02v
Standard_D4as_v5	4	2	FG-VM04 or FG-VM04v
Standard_D8as_v5	8	4	FG-VM08 or FG-VM08v
Standard_D16as_v5	16	8	FG-VM16 or FG-VM16v
Standard_D32as_v5	32	8	FG-VM32 or FG-VM32v
DadsV5 Series			
Standard_D2ads_v5	2	2	FG-VM02 or FG-VM02v
Standard_D4ads_v5	4	2	FG-VM04 or FG-VM04v
Standard_D8ads_v5	8	4	FG-VM08 or FG-VM08v
Standard_D16ads_v5	16	8	FG-VM16 or FG-VM16v
Standard_D32ads_v5	32	8	FG-VM32 or FG-VM32v

ARM Ampere Altra

This series contains support for Ampere Altra ARM-based processor delivering a high price-to-performance ratio for general purpose workloads.

Dpsv5 and Dpdsv5-series

Instance Type	vCPU	Max NIC	Recommended BYOL license
Dpsv5 Series			
Standard_D2ps_v5	2	2	FG-VM02 or FG-VM02v
Standard_D4ps_v5	4	2	FG-VM04 or FG-VM04v
Standard_D8ps_v5	8	4	FG-VM08 or FG-VM08v
Standard_D16ps_v5	16	4	FG-VM16 or FG-VM16v
Standard_D32ps_v5	32	8	FG-VM32 or FG-VM32v
Dpdsv5 Series			

Instance Type	vCPU	Max NIC	Recommended BYOL license
Standard_D2pds_v5	2	2	FG-VM02 or FG-VM02v
Standard_D4pds_v5	4	2	FG-VM04 or FG-VM04v
Standard_D8pds_v5	8	4	FG-VM08 or FG-VM08v
Standard_D16pds_v5	16	4	FG-VM16 or FG-VM16v
Standard_D32pds_v5	32	8	FG-VM32 or FG-VM32v

Dplsv5 and Dpldsv5-series

Instance Type	vCPU	Max NIC	Recommended BYOL License
Dplsv5 Series			
Standard_D2pls_v5	2	2	FG-VM02 or FG-VM02v
Standard_D4pls_v5	4	2	FG-VM04 or FG-VM04v
Standard_D8pls_v5	8	4	FG-VM08 or FG-VM08v
Standard_D16pls_v5	16	4	FG-VM16 or FG-VM16v
Standard_D32pls_v5	32	8	FG-VM32 or FG-VM32v
Dpldsv5 Series			
Standard_D2plds_v5	2	2	FG-VM02 or FG-VM02v
Standard_D4plds_v5	4	2	FG-VM04 or FG-VM04v
Standard_D8plds_v5	8	4	FG-VM08 or FG-VM08v
Standard_D16plds_v5	16	4	FG-VM16 or FG-VM16v
Standard_D32plds_v5	32	8	FG-VM32 or FG-VM32v

Epsv5 and Epdsv5-series

Instance Type	vCPU	Max NIC	Recommended BYOL License
Epsv5 Series			
Standard_E2ps_v5	2	2	FG-VM02 or FG-VM02v
Standard_E4ps_v5	4	2	FG-VM04 or FG-VM04v
Standard_E8ps_v5	8	4	FG-VM08 or FG-VM08v
Standard_E16ps_v5	16	4	FG-VM16 or FG-VM16v
Standard_E32ps_v5	32	8	FG-VM32 or FG-VM32v

Instance Type	vCPU	Max NIC	Recommended BYOL License
Epdsv5 Series			
Standard_E2pds_v5	2	2	FG-VM02 or FG-VM02v
Standard_E4pds_v5	4	2	FG-VM04 or FG-VM04v
Standard_E8pds_v5	8	4	FG-VM08 or FG-VM08v
Standard_E16pds_v5	16	4	FG-VM16 or FG-VM16v
Standard_E32pds_v5	32	8	FG-VM32 or FG-VM32v

Region support

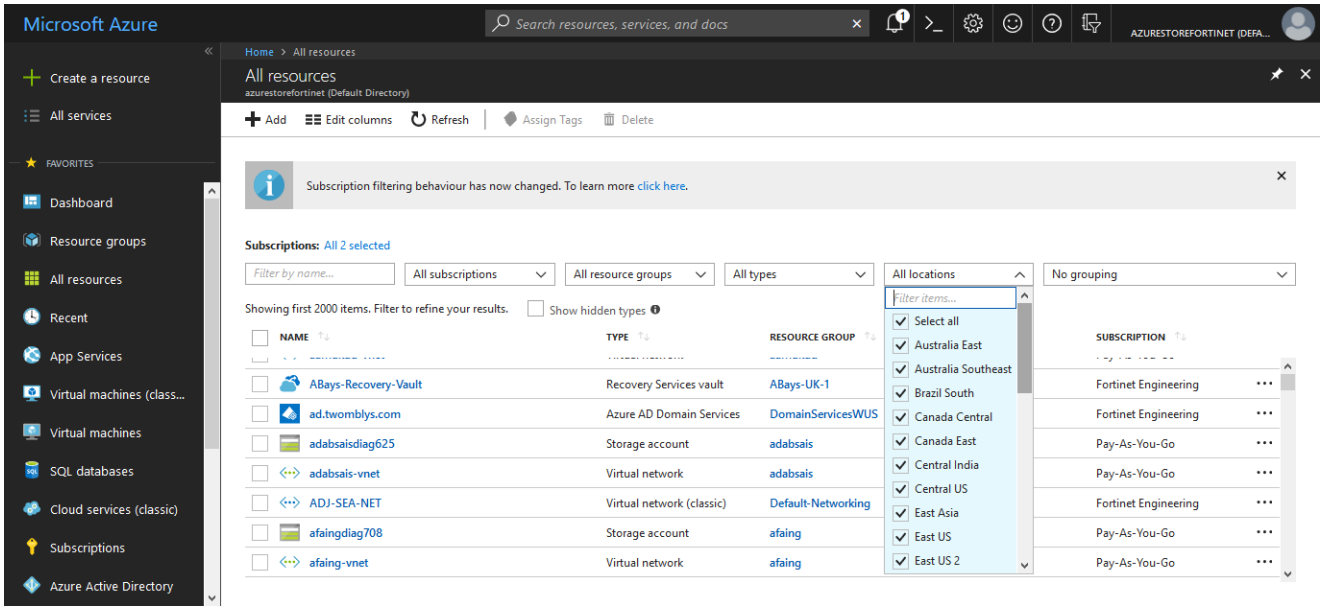
Azure region support can mean one of the following:

- FortiGate-VM is available for purchase in a specific region.
- You can deploy FortiGate-VM on the datacenter located in the chosen region within the Azure portal. They are the “locations".
- You can deploy FortiGate-VM on regional Azure, such as in China, Germany, and U.S. Gov. Each has its own URL domain.

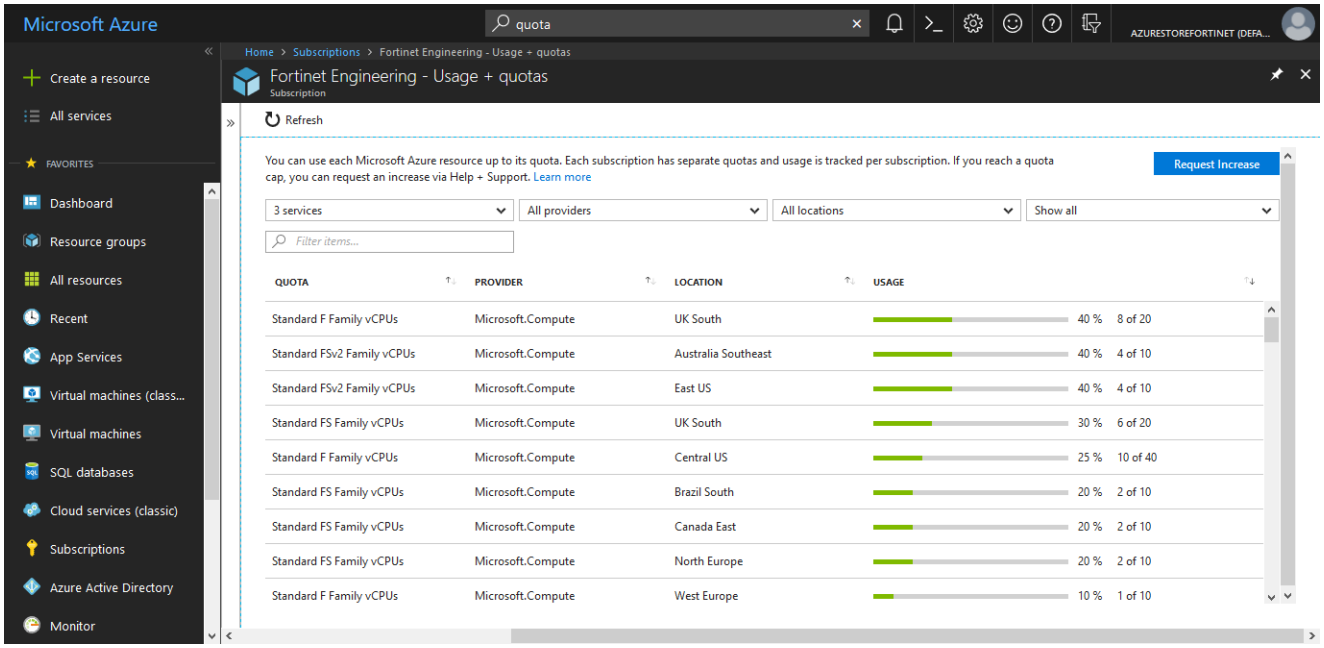
FortiGate-VM is available for purchase in all regions where Azure is commercially available. See the Azure pricing FAQ.

In terms of the location where you deploy FortiGate-VM, ensure that quota is available. Some limits, such as VM cores, exist at a regional level. See Azure subscription and service limits, quotas, and constraints. You can also request that Microsoft increase VM cores if necessary, as Increase regional vCPU quotas explains. Choose the instance types supported to deploy FortiGate-VM (Instance type support on page 6).

Locations



Azure regional quota for vCPU cores



Models

FortiGate-VM is available with different CPU and RAM sizes and you can deploy it on various private and public cloud platforms. The following table shows the models conventionally available to order, also known as bring your own license models. See Order types on page 15.

Model name	vCPU minimum	vCPU maximum
FG-VM01/01v/01s	1	1
FG-VM02/02v/02s	1	2
FG-VM04/04v/04s	1	4
FG-VM08/08v/08s	1	8
FG-VM16/16v/16s	1	16
FG-VM32/32v/32s	1	32
FG-VMUL/ULv/ULs	1	Unlimited

With the changes in the FortiGuard extended IPS database introduced in FortiOS 7.4.0, some workloads that depend on the extended IPS database must have the underlying VM resized to 8 vCPU or more to continue using the extended IPS database.

See Support full extended IPS database for FortiGate VMs with eight cores or more.

For information about changing the instance type on an existing VM, see Change the size of a virtual machine.

For more information about the VM series, see Virtual Machine series.

The v-series and s-series do not support virtual domains (VDOMs) by default. To add VDOMs, you must separately purchase perpetual VDOM addition licenses. You can add and stack VDOMs up to the maximum supported number after initial deployment.

Generally, there are RAM size restrictions to FortiGate-VM BYOL licenses. However, these restrictions do not apply to Azure deployments. Azure allows any RAM size with certain CPU models. Licenses are based on the number of CPUs (the number of vCPU cores for Azure) only.

Previously, platform-specific models such as FortiGate-VM for Azure with an Azure-specific orderable menu existed. However, the common model now applies to all supported platforms.

For information about each model's order information, capacity limits, and adding VDOMs, see the FortiGate-VM datasheet.

The primary requirement for provisioning a virtual FortiGate may be the number of interfaces it can accommodate rather than its processing capabilities. In some cloud environments, options with a high number of interfaces tend to have high numbers of vCPUs.

The licensing for FortiGate-VM does not restrict whether the FortiGate can work on a VM instance in a public cloud that uses more vCPUs than the license allows. The number of vCPUs that the license indicates does not restrict the FortiGate-VM from working, regardless of how many vCPUs the virtual instance includes. However, only the licensed number of vCPUs process traffic and management tasks. The FortiGate-VM does not use the rest of the vCPUs.

The following shows an example for FGT-VM08:

License	1 vCPU	2 vCPU	4 vCPU	8 vCPU	16 vCPU	32 vCPU
FGT-VM08	OK	OK	OK	OK	The FortiGate-VM uses eight vCPUs used for traffic and management. It does not use the rest.	The FortiGate-VM uses eight vCPUs used for traffic and management. It does not use the rest.

You can provision a VM instance based on the number of interfaces you need and license the FortiGate-VM for only the processors you need.

Licensing

You must have a license to deploy FortiGate-VM for Azure:

Order types

On Azure, there are usually two order types: bring your own license (BYOL) and pay as you go (PAYG).

BYOL offers perpetual (normal series and v-series) and annual subscription (s-series) licensing as opposed to PAYG, which is an hourly subscription available with marketplace-listed products. 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.

With a PAYG subscription, the FortiGate-VM becomes available for use immediately after you create the instance. The marketplace product page mentions term-based prices (hourly or annual).

In BYOL and PAYG, Azure charges separately for resource consumption on computing instances, storage, and so on, without the use of software running on top of it (in this case FortiGate).

For BYOL, you typically order a combination of products and services, including support entitlement. S-series SKUs contain the VM base and service bundle entitlements for easier ordering. PAYG includes support, for which you must contact Fortinet Support with your customer information. See Plans.

To purchase PAYG, all you need to do is subscribe to the product on the marketplace. However, you must contact Fortinet Support with your customer information to obtain support entitlement. See Creating a support account on page 16.

PAYG FortiGate-VM instances do not support the use of virtual domains (VDOMs). If you plan to use VDOMs, deploy BYOL instances instead.

PAYG and BYOL licensing and payment models are not interchangeable. For example, once you spin up a FortiGate-VM PAYG instance, you cannot inject a BYOL license on the same VM. Likewise, you cannot convert a FortiGate-VM BYOL instance to PAYG.

Creating a support account

FortiGate-VM for Azure supports pay as you go (PAYG) and bring your own license licensing models. See Order types on page 15.

PAYG users do not need to register from the FortiGate GUI. If you are using a PAYG licensing model and need to ask technical questions to support, obtain support entitlement by contacting Fortinet Customer Support after creating the FortiGate-VM instance in Azure, and by providing the following information:

- Your FortiGate-VM instance's serial number
- Your Fortinet account's email ID. If you do not have a Fortinet account, you can create one at Customer Service & Support.

BYOL

You must obtain a license to activate the FortiGate-VM. If you have not activated the license, you see the license upload screen when you log into the FortiGate-VM and cannot proceed to configure the FortiGate-VM.

You can obtain licenses for the bring your own license (BYOL) licensing model through any Fortinet partner. If you do not have a partner, contact azuresales@fortinet.com for assistance in purchasing a license.

After you purchase a license or obtain an evaluation license, you receive a PDF with an activation code.

The FortiOS permanent trial license requires a FortiCare account. This trial license has limited features and capacity. The trial license only applies to BYOL deployments for FortiGate-VM on Azure. See Permanent trial mode for FortiGate-VM for details.

To register a BYOL license:

1. Go to Customer Service & Support and create a new account or log in with an existing account.
2. Click *Register Now* to start the registration process.
3. In the *Registration Code* field, enter your license activation code, then select *Next* to continue registering the product.
4. If you register the S-series subscription model, the site prompts you to select one of the following:
   - Click *Register* to newly register the code to acquire a new serial number with a new license file.
   - Click *Renew* to renew and extend the licensed period on top of the existing serial number, so that all features on the VM node continue working uninterrupted upon license renewal.
5. At the end of the registration process, download the license (.lic) file to your computer. You upload this license later to activate the FortiGate-VM. After registering a license, Fortinet servers may take up to 30 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiGate-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

PAYG

To register a PAYG license:

1. Deploy and boot the FortiGate-VM pay as you go instance and log into the FortiGate-VM GUI management console.
2. From the Dashboard, copy the VM's serial number.
3. Go to Customer Service & Support and create a new account or log in with an existing account.
4. Go to *Asset* > *Register/Activate* to start the registration process.
5. In the *Registration* page, enter the serial number, and select *Next* to continue registering the product.
6. After completing registration, contact Fortinet Customer Support and provide your FortiGate-VM instance's serial number and the email address associated with your Fortinet account.

Verifying the license type

You can run the `get system status` command. For a bring your own license (BYOL) instance, the output is as follows:

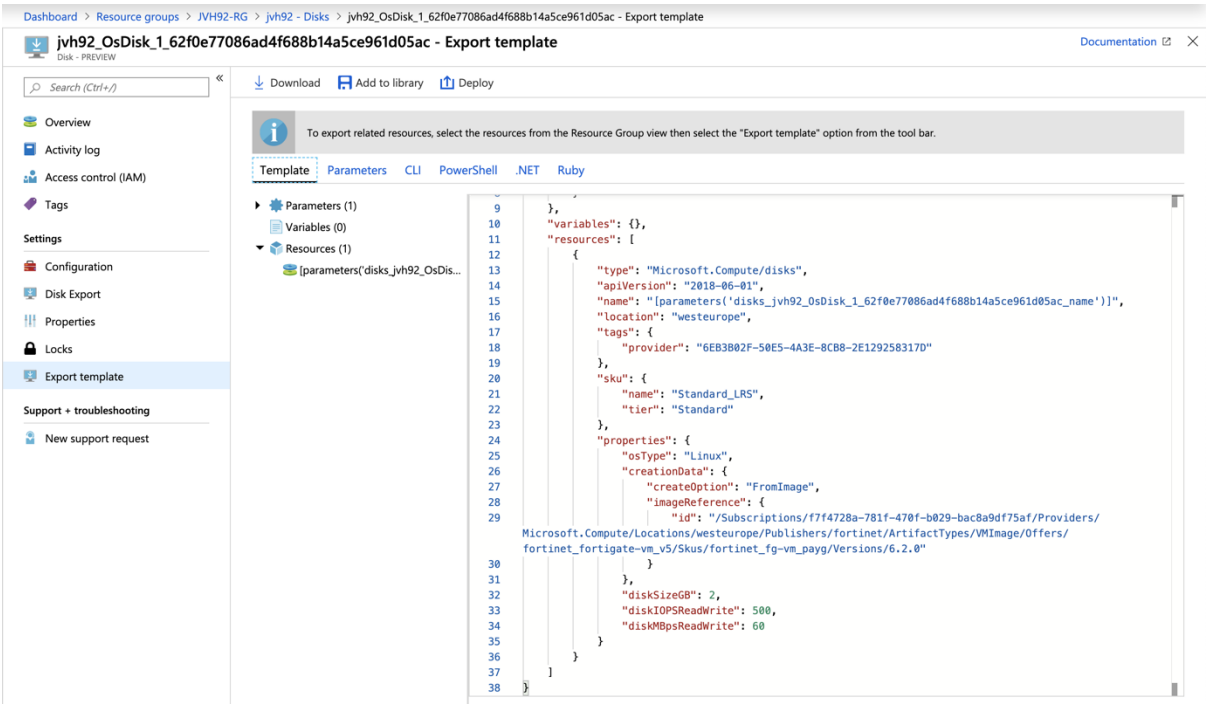
```
Version: FortiGate-VM64-AZURE v7.6.0,buildXXXX,200330 (GA)
```

For a pay as you go (PAYG) instance, the output is as follows:

```
Version: FortiGate-VM64-AZUREONDEMAND v7.6.0,buildXXXX,200330 (GA)
```

By opening the operating system (OS) disk, you can also verify the image used during deployment, which indicates the license type. The deployment process clones the disk from a disk image that Fortinet has provided to the Azure marketplace.

Open your deployed VM's OS disk and select *Export template*. In the template, search for `imageReference`. For a BYOL instance, this URI contains `fortinet_fg-vm`. For a PAYG instance, it contains `fortinet_fg-vm_payg_20190624`.



Migrating a FortiGate-VM instance between license types

When deploying a FortiGate-VM on public cloud, you determine the license type (pay as you go (PAYG) or bring your own license (BYOL)) during deployment. The license type is fixed for the VM's lifetime. The image that you use to deploy the FortiGate-VM on the public cloud marketplace predetermines the license type.

Migrating a FortiGate-VM instance from one license type to another requires a new deployment. You cannot simply switch license types on the same VM instance. However, you can migrate the configuration between two VMs running as different license types. There are also FortiOS feature differences between PAYG and BYOL license types. For example, a FortiGate-VM PAYG instance is packaged with unified threat management protection and does not support virtual domains, whereas a FortiGate-VM BYOL instance supports greater protection levels and features depending on its contract.

To migrate FortiOS configuration to a FortiGate-VM of another license type:

1. Connect to the FortiOS GUI or CLI and back up the configuration. See Configuration backups.
2. Deploy a new FortiGate-VM instance with the desired license type. You can deploy the instance using one of the following methods:
   - Azure marketplace
   - Azure CLI
   - Deploying FortiGate-VM using Azure PowerShell on page 34
   - ARM templates
   - Terraform templates

   If deploying a BYOL instance, you must purchase a new license from a Fortinet reseller. You can apply the license after deployment via the FortiOS GUI or bootstrap the license and configuration during initial bootup using custom data as described in Bootstrapping the FortiGate CLI and BYOL license at initial bootup using user data on page 39.
3. Restore the configuration on the FortiGate-VM instance that you deployed in step 2. As with the license, you can inject the configuration during initial bootup. Alternatively, you can restore the configuration in the FortiOS GUI as described in Configuration backups.
4. If you deployed a PAYG instance in step 2, register the license. To receive support for a PAYG license, you must register the license as described in Creating a support account on page 16.

Obtaining a FortiCare-generated license for Azure on-demand instances

New Azure on-demand and upgraded instances can retrieve a FortiGate serial number and license from FortiCare servers. Using the serial number, you can register the device to their account and start using FortiToken and FortiGate Cloud services.

The FortiGate-VM must be able to reach FortiCare to receive a valid on-demand license. Ensure connectivity to FortiCare (https://directregistration.fortinet.com/) by checking all related setup on the virtual network, subnet, network security group, route table, public IP addresses, and so on.

To verify cloudinit automatically obtained a license for a newly-deployed instance:

```
# diagnose debug cloudinit show
 >> Load VM metadata document
 >> Requesting FortiCare license: FGTAZRXXXXXXXXXX
 >> VM license install succeeded. Rebooting firewall.

# diagnose debug vm-print-license
```

```
SerialNumber: FGTAZRXXXXXXXXX
CreateDate: Wed Jul 29 16:48:34 2020
Key: yes
Cert: yes
Key2: yes
Cert2: yes
Model: PG (20)
CPU: 2147483647
MEM: 2147483647


# execute vm-license
PAYG license exists.
```

If in a closed network, the command execution resembles the following, as the `execute vm-license` command attempts to get a license from FortiCare:

```
# diagnose debug cloudinit show

# diagnose debug vm-print-license
SerialNumber: FGTAZRXXXXXXXXX
CreateDate: 1597362903
Model: PG (20)
CPU: 2147483647
MEM: 2147483647

# execute vm-license
This operation will reboot the system !
Do you want to continue? (y/n)


Load VM metadata document
Requesting FortiCare license: FGTAZRXXXXXXXXX
```

If the FortiGate-VM connects to FortiCare successfully, the following message displays.

```
VM license install succeeded. Rebooting firewall.
```

To obtain a license for an upgraded instance or instance from a closed network:

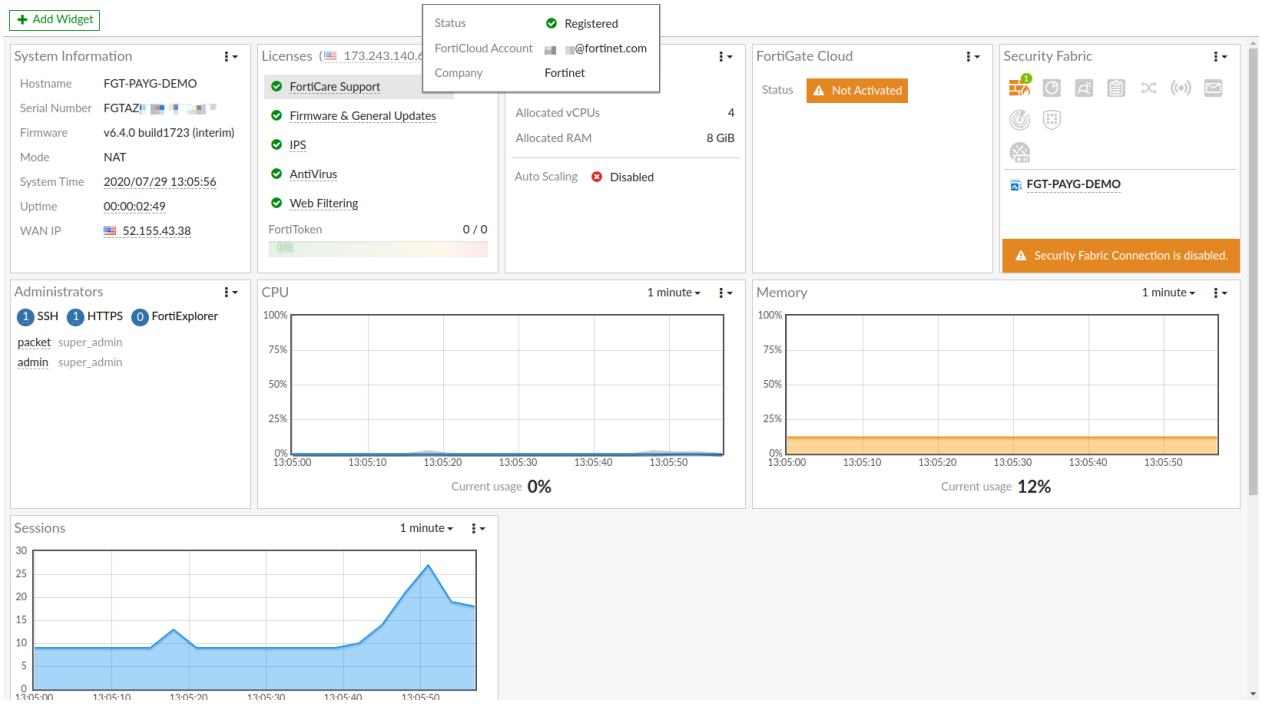
If you created the FortiGate-VM in a closed environment or it cannot reach FortiCare, the FortiGate-VM self-generates a local license. You can obtain a FortiCare license, ensure that the FortiGate-VM can connect to FortiCare, then run the `execute vm-license` command to obtain the license from FortiCare.

```
# execute vm-license
This operation will reboot the system !
Do you want to continue? (y/n)y

Load VM metadata document
Requesting FortiCare license: FGTAZRXXXZXXXXXX
VM license install succeeded. Rebooting firewall.
```

To register the serial number:

1. Register the license using the serial number in FortiCare (see Creating a support account on page 16).
2. Obtain the VM ID:
   - In FortiOS, run one of the following commands:
     - `diagnose test application azd 6` and search for the `VM Instance ID`
     - `get system instance-id`
   - In Azure, run `az vm show -g Resource-Group-Name -n PAYG-VM-Name --query vmId -o tsv`. It may take up to an hour for the registration status to synchronize and update in the FortiOS GUI.
3. Go *Dashboard* > *Status* and in the *Licenses* widget verify the *FortiCare Support* status.



4. Once the registration is complete, you can log in to a FortiGate Cloud account and download the two free tokens that come standard with FortiGates (see FortiTokens).

Deploying FortiGate-VM on Azure

You can deploy FortiGate-VM next generation firewall for Azure as a virtual appliance in Azure cloud (infrastructure as a service). See Single FortiGate-VM deployment on page 134.

Azure services and components

FortiGate-VM for Azure is a Linux VM instance. The following table lists Azure services and components that you need to understand when deploying FortiGate-VM. All services and components listed relate to ordinary FortiGate-VM single instance deployment or FortiGate-native active-passive HA deployment.

Service/component	Description
Azure Virtual Network (VNet)	This is where the FortiGate-VM and protected VMs are situated and users control the network. When you deploy FortiGate-VM, you can configure relevant network settings.
VM	FortiGate-VM for Azure is a customized Linux VM instance.
Subnets, route tables	You must appropriately configure the FortiGate-VM with subnets and route tables to handle traffic. When deploying from the marketplace launcher, there are two subnets for the FortiGate-VM labeled `PublicFacingSubnet` and `InsideSubnet` by default.
Resource group	A group of resources where the FortiGate-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 FortiGate-VM to access and manage it over the Internet.
Security groups	Unlike AWS, you cannot configure Azure security groups at the time of FortiGate-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 FortiGate-VM from the marketplace launcher, you do not need VHD files. However, you can launch FortiGate-VM (BYOL) directly from the FortiGate-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.
ARM Templates	You can deploy FortiGate-VM instances in two ways: 1. Find the FortiGate-VM product listing on the marketplace and launch from it. You do not necessarily see Azure Resource Manager (ARM) templates onscreen but they are used on the backend. You can also download the templates once the deployment process proceeds.

Service/component	Description
	2. Launch custom deployment in the Azure portal. Upload ARM templates of your choice that deploy FortiGate with your desirable topology and configuration. ARM templates are available on GitHub. Fortinet-provided ARM templates are not supported within the regular Fortinet technical support scope. Contact azuresales@fortinet.com with questions.
Load Balancer	A network LB automatically distributes traffic across multiple FortiGate-VM instances when configured properly. Topologies differ depending on how you distribute incoming and outgoing traffic. Fortinet provides a FortiGate marketplace product listing that automatically comes along with 2 FortiGate-VM nodes and LB. See HA for FortiGate-VM on Azure on page 145.

Deploying FortiGate-VM from a VHD image file

You can deploy FortiGate-VM x64 and ARM64 images in Azure:

- Deploying FortiGate-VM x64 from a VHD image file on page 22
- Deploying FortiGate-VM ARM64 from a VHD image file on page 23

Deploying FortiGate-VM x64 from a VHD image file

You can deploy a x64-based FortiGate-VM from VHD image files using custom templates or Azure CLI.

FortiGate-VM VHD image files are available from Fortinet Customer Service & Support.

To download the FortiGate VHD image file and upload it:

1. Go to *Download* > *VM Image*.
2. From the *Product* dropdown list, select *FortiGate*.
3. From the *Platform* dropdown list, select *Azure*.
4. Download the FGT_VM64_AZURE-v7-buildXXXX-FORTINET.out.hyperv.zip file, where XXXX is the build number.
5. Unzip the file.
6. Locate the fortios.vhd file.
7. Upload the fortios.vhd file to the blob/storage location as your deployment templates require.

Fortinet Customer Service & Support hosts only two minor versions for the two latest major FortiOS versions. To obtain older files, go to *Download* > *Firmware Images*, select *FortiGate* as the *Product*, then go to the *Download* tab. Go to the desired version and download the FGT_VM64_AZURE-v7-buildXXXX-FORTINET.out.hyperv.zip file.

See How do I create a VM from a generalized vhd?.

Deploying FortiGate-VM ARM64 from a VHD image file

You can deploy FortiGate-VM ARM64 images via the Azure Compute Gallery.

Downloading the FortiGate image

FortiGate-VM VHD image files are available from Fortinet Customer Service & Support.

To download the FortiGate VHD image file and upload it:

1. Go to *Download* > *VM Image*.
2. From the *Product* dropdown list, select *FortiGate*.
3. From the *Platform* dropdown list, select *Azure*.
4. Download the FGT_ARM64_AZURE-v7-buildXXXX-FORTINET.out.hyperv.zip file, where XXXX is the build number.
5. Unzip the file.
6. Locate the fortios.vhd file.
7. Upload the fortios.vhd file to the blob/storage location.

Fortinet Customer Service & Support hosts only two minor versions for the two latest major FortiOS versions. To obtain older files, go to *Download* > *Firmware Images*, select *FortiGate* as the *Product*, then go to the *Download* tab. Go to the desired version and download the FGT_ARM64_AZURE-v7-buildXXXX-FORTINET.out.hyperv.zip file.

Creating Azure Compute Gallery from the Azure portal

See Store and share images in an Azure Compute Gallery. You can also create a Compute Gallery via the Azure CLI. See Create a gallery for storing and sharing resources.

Creating an image definition

You can create an image definition via the Azure portal or CLI. 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 uploaded to the storage account in Downloading the FortiGate image on page 23.

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

Deploying FortiGate with a custom ARM template

You can deploy a FortiGate-VM (BYOL) outside the marketplace product listing using a custom ARM template in the Azure portal. This is an alternative method for if you want to deploy FortiGate-VM on instance types/sizes that you cannot find on the FortiGate-VM marketplace launcher. Some instance types of your choice may not properly boot up or run due to lack of official FortiGate-VM instance support.

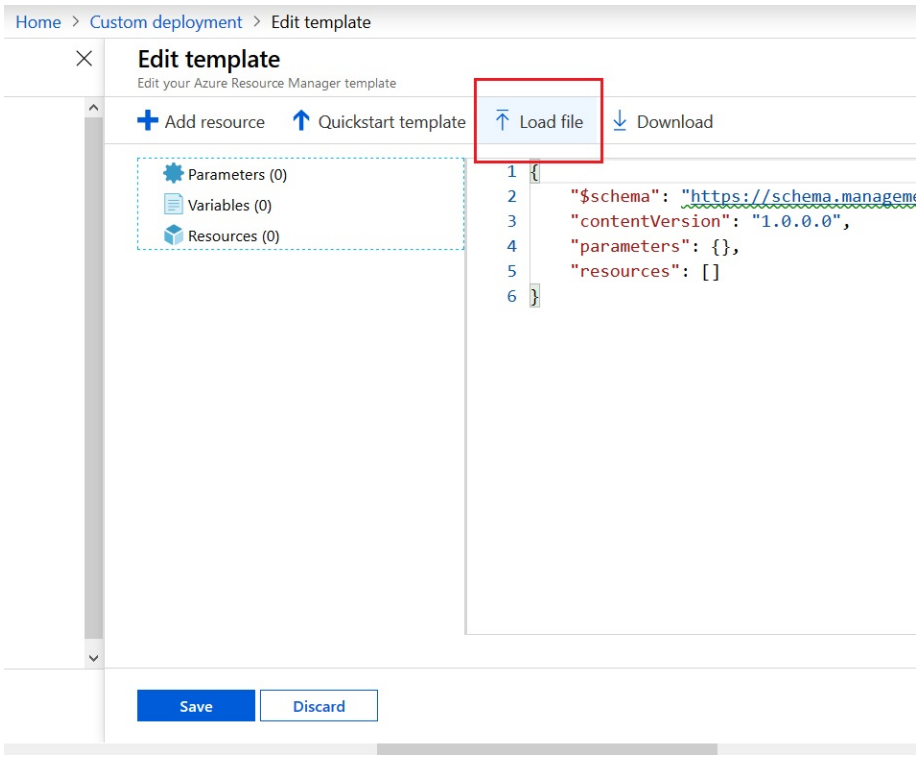
There is a bare minimum set of templates available for your deployment.

You can also specify bootstrapping FortiGate CLI commands within the template and run them at the time of initial bootup.

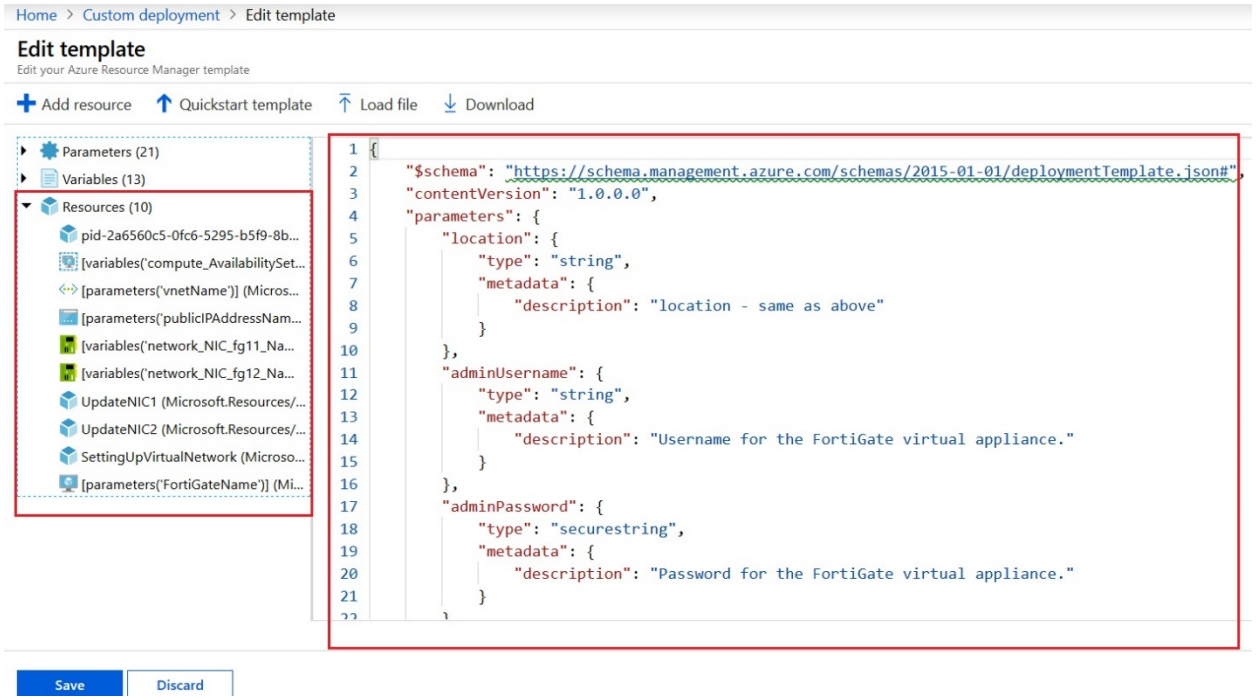
Invoking a custom ARM template

To invoke a custom ARM template:

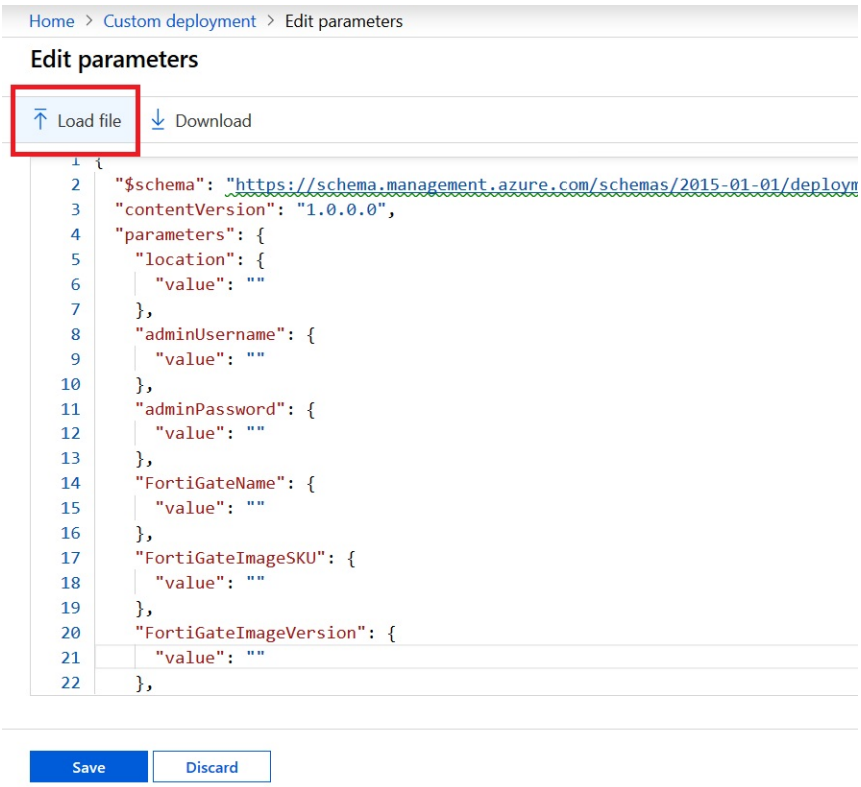
1. Log in to the Azure portal and go to *Custom deployment*.
2. Click *Build your own template in the editor*.
3. From GitHub, copy and paste the template content, or download the template file and load it into the *Edit template* window.



4. Ensure that the template is shown in the screen. Click *Save*.



5. Edit the parameters:
   a. Click *Edit parameters*.
   b. Copy and paste the parameters from GitHub, or download the file as in step 3. You can manually edit the fields.



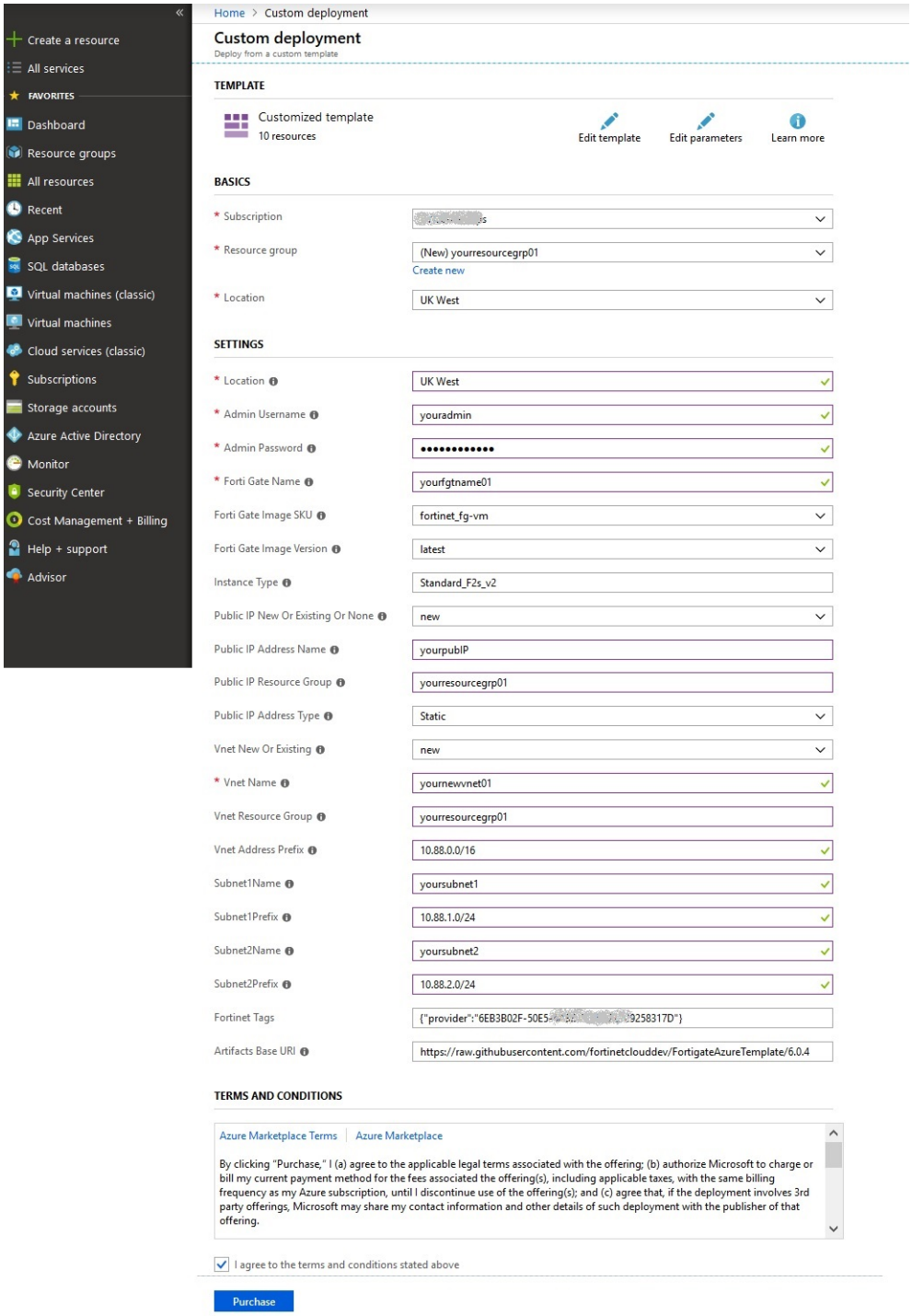
c. Click *Save*.

6. Complete the following fields:

Field	Description
Basics	
Subscription	Enter the subscription that is entitled to purchase marketplace products of your choice. Generally, selecting a subscription that your organization has configured to not be able to purchase Azure resources is advisable. Ensure that you specify the appropriate subscription.
Resource Group	You must create a new resource group. Click *Create New* and enter a nonexistent resource group.
Location	From the dropdown list, select a region to deploy the FortiGate-VM and related resources.
Settings	
Location	Manually specify the same location as the above by entering the region.
Admin Username	Specify an administrator login name that can log into the FortiGate management console. Azure does not allow names such as root or admin.
Admin Password	Specify an administrator password with some character complexity. The password must be between 12 and 72 characters and contain at least three of the following: one lower-case character, one upper-case character, one number, and one special character.

Field	Description
FortiGate Name	Specify the FortiGate-VM instance name or FortiGate hostname that can be identified on the Azure portal.
FortiGate Image SKU	Leave this as-is.
FortiGate Image version	Select a version. This version points to the one that the FortiGate marketplace listing supports. As the template may contain obsolete versions, specifying *Latest* is recommended.
Instance Type	Choose an instance type based on the number of virtual CPU cores. Recommended types are the following compute instances: • Standard_F1 • Standard_F2 • Standard_F4 • Standard_F8 • Standard_F1s • Standard_F2s • Standard_F4s • Standard_F8s • Standard_F16s • Standard_F2s_v2 • Standard_F4s_v2 • Standard_F8s_v2 • Standard_F16s_v2 • Standard_F32s_v2 • Standard_F64s_v2 • Standard_F72s_v2 Instances with over 32 vCPU requires a FG-VMUL license that can support an unlimited number of CPU cores.
Public IP New or Existing or None	Choose *New*.
Public IP Address Name	Enter a name to distinguish the public IP address.
Public IP Resource Group	Ensure you specify the same resource group as entered in *Basics* > *Resource Group* above.
Public IP Address Type	Select *Static*.
Vnet New or Existing	Select *New*.
Net Name	Specify the same name as the resource group name.
Vnet Address Prefix	Specify a CIDR that does not overlap with your existing Vnet CIDRs.
Subnet1Name	Enter a name to distinguish the public subnet.
Subnet1Prefix	Specify a CIDR that belongs to the Vnet Address Prefix above.
Subnet2Name	Enter a name to distinguish the private/protected subnet.

Field	Description
Subnet2Prefix	Specify another CIDR that belongs to the Vnet Address Prefix above.
Fortinet Tags	Leave as-is.
Artifacts Base URL	Leave as-is.

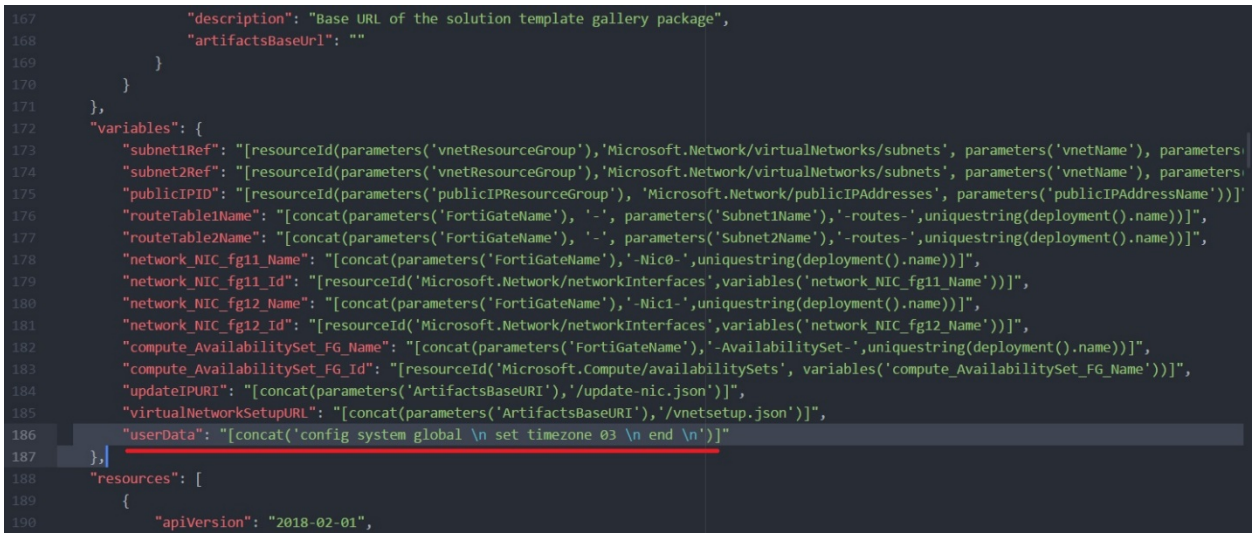


7. Select the *I agree to the terms and conditions stated above* checkbox. Click *Purchase*. It takes about 10-15 minutes to deploy the FortiGate-VM and related resources. If you encounter an issue, resolve the issue and retry the deployment.
8. After successful deployment, connect to the FortiGate instance using the credentials specified above. See Connecting to the FortiGate-VM on page 137.

Bootstrapping the FortiGate CLI at initial bootup using user data

You can run FortiGate CLI commands at initial bootup by using custom cloud-init.

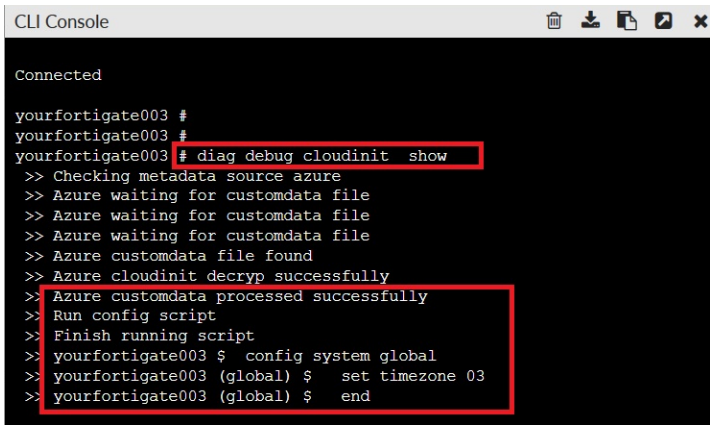
1. Download the ARM template and open in a text editor.
2. Find the variables section and the userData statement as shown. The line number may be different than in the screenshot.
3. After concat, specify FortiGate CLI commands. If they are run across multiple lines (in the FortiGate CLI, these commands are run by using the *Enter* key), separate each line with a backslash and n and enclose the whole statement with single quotes.



The example above is the same as executing the following in the FortiGate CLI:

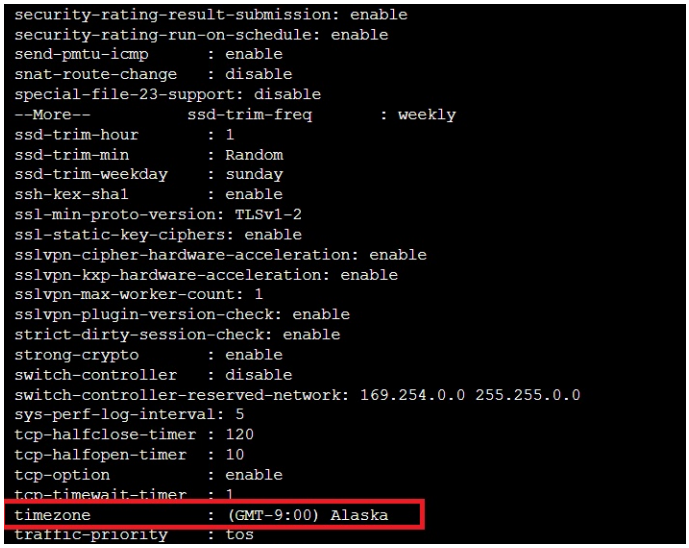
```
config system global
   set timezone 03
end
```

4. Load the file as shown in Invoking a custom ARM template on page 24.
5. After deployment, log into the FortiGate.
6. Check if the command was successfully run:
   a. In the CLI console, enter `diag debug cloudinit show`. If the cloud-init was successful, the CLI shows `Azure customdata processed successfully`. The FortiGate CLI command syntax must be correct.



If the CLI command fails, you see an error message with `diag debug cloudinit show` as above. Resolve it and try again.

b. Check the timezone by running `config system global` and `get` commands.



As expected, the timezone was changed. This means the bootstrapping CLI command worked.

Bootstrapping the FortiGate CLI and BYOL license at initial bootup using user data

You can run FortiGate CLI commands and a BYOL license at initial bootup by using custom cloud-init. Use the following sample ARM templates:

- Template
- Parameters

For details on using a custom ARM template, see Deploying FortiGate with a custom ARM template on page 24.

First, you must create two text files: one for FortiGate CLI configuration and another for a license file.

1. Create a CLI configuration file:
   a. In a text editor, create a text file that contains CLI commands like the following:

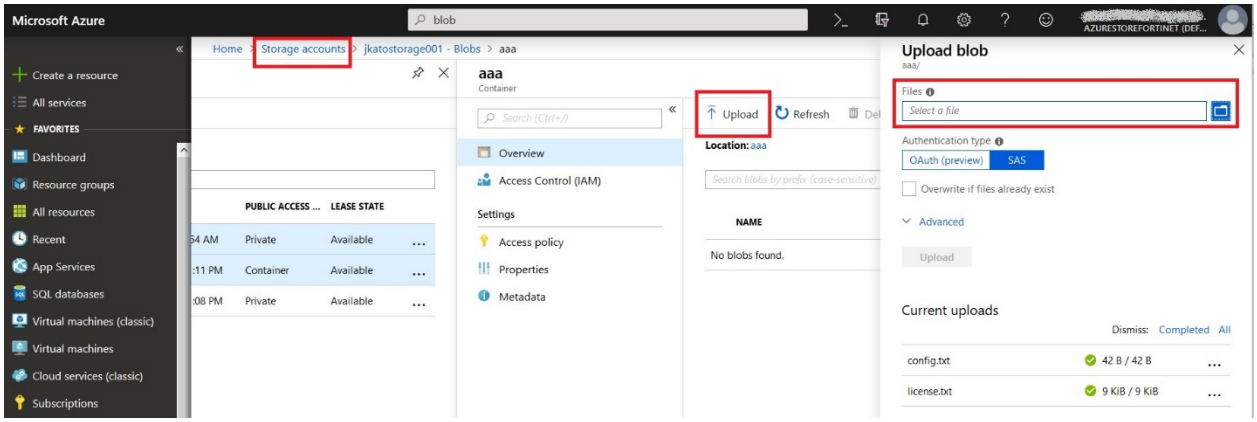
```
config system global
   set timezone 03
end
```

b. Save the file as config.txt or another desired name. This example sets the timezone as GMT-9 Alaska.

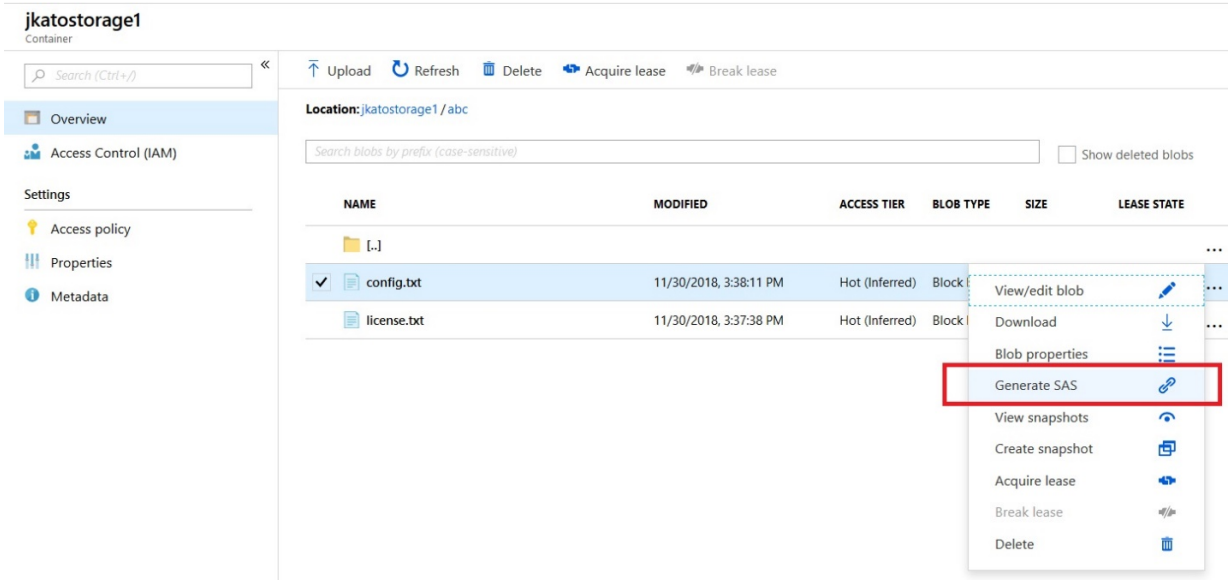
2. Create a license text file:
   a. Download a FortiGate license from Customer Service & Support and save the file as license.txt or any other desired name. The file contains content that resembles the following:

3. Place both text files on your Azure blob.
4. In this example, you are required to have the following:
   - Storage account
   - Private container in the blob

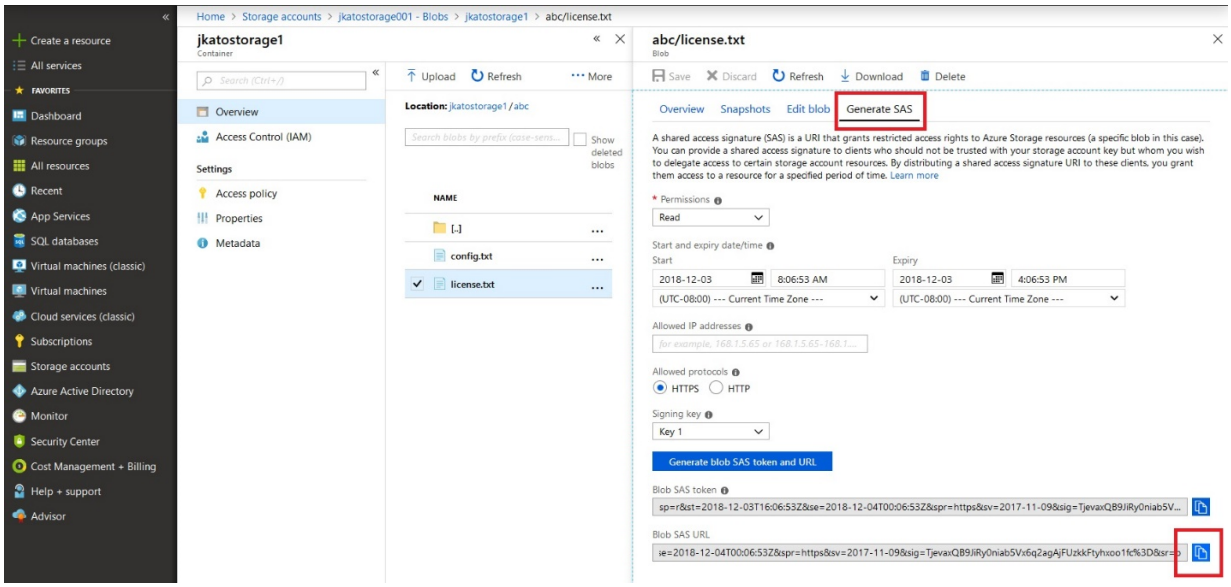
   Upload the two text files in a folder with authentication type SAS.



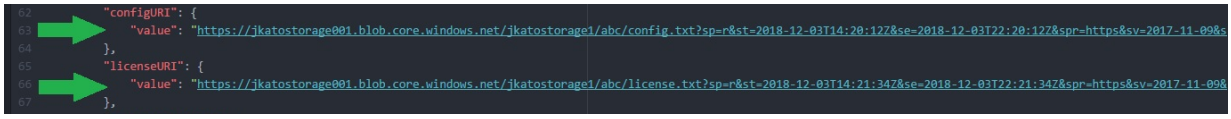
5. Copy and paste the SAS URLs into the parameters file:
   a. After uploading, click the menu icon beside config.text. Click *Generate SAS* to create an SAS URL link. Repeat this step with the license.txt file.



b. Copy the SAS URLs.



c. Paste the SAS URLs into the `configURI` and `licenseURI` sections of the parameters-BYOL-CLI-and-license-json file as shown:



6. Review all template fields. Ensure the following:

a. Your chosen subscription is entitled to purchase the marketplace product.

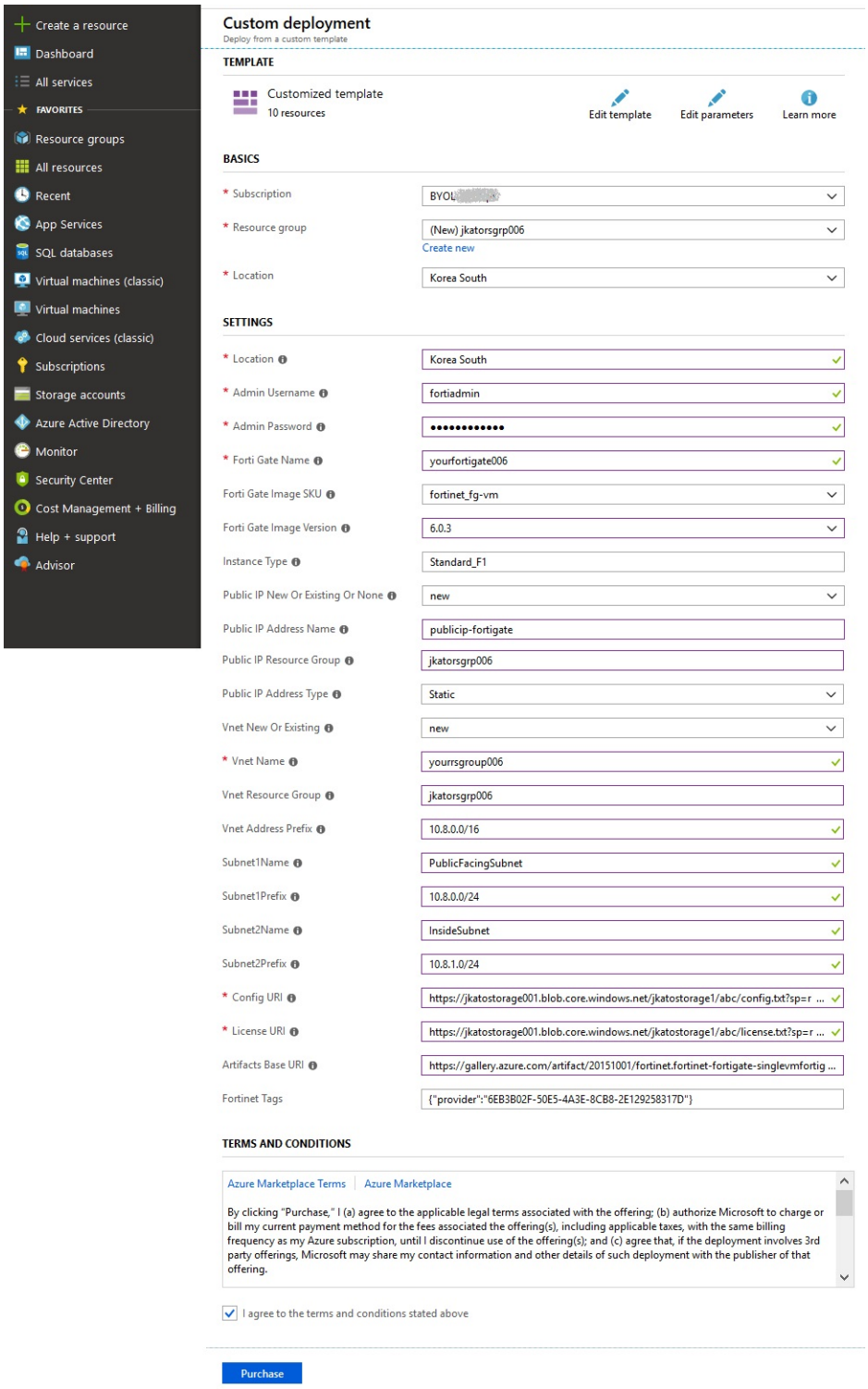
b. The same location is entered under *Settings* and under *Basics*. Ensure that the location has sufficient quota to accommodate the FortiGate-VM with the desired number of CPU cores. For details, see Region support on page 12.

c. A new resource group is created and the same name is entered under *Public IP Resource Group* and *Vnet Resource Group*.

d. The *Fortinet Tags* field is automatically populated. There is no need to manually input information into this field. If this field is empty or shows an error, reload the browser, then load the template and parameter files again.

e. The license and config files' SAS URLs are not expired.

Once all fields are entered, the template should resemble the following:



7. Select the checkbox to agree to the terms, then click *Purchase*.

8. After deployment is complete, log into the FortiGate by accessing *https://<IP_address>* in your browser.
9. If the license was successfully loaded, you should see the dashboard. If you are prompted to upload a license, this means that bootstrapping the license failed. In this case, you can manually upload the license file, and once the system completes rebooting, log in and invoke the CLI from the dashboard. To check why bootstrapping failed, run the `diag debug cloudinit show` command. See Bootstrapping the FortiGate CLI at initial bootup using user data on page 29.

```
yourfortigate030 # diag debug cloudinit show
 >> Checking metadata source azure
 >> Azure waiting for customdata file
 >> Azure waiting for customdata file
 >> Azure waiting for customdata file
 >> Azure customdata file found
 >> Azure cloudinit decryp successfully
 >> Azure Fos-instance-id: 9106ebee-4840-443f-b951-2993af73cd3a
 >> Azure couldn't find mime link
 >> Azure trying to get license from: https://jkatostorage001.blob.core
 >> Azure download license successfully
 >> Azure trying to get config script from https://jkatostorage001.blob
 >> Azure download config script successfully
 >> Azure customdata processed successfully
 >> Run config script
 >> Finish running script
 >> yourfortigate030 $  config system global
 >> yourfortigate030 (global) $  set timezone 03
 >> yourfortigate030 (global) $  end
```

Deploying FortiGate-VM using Azure PowerShell

You can deploy FortiGate-VM (BYOL) outside the marketplace product listing using Azure PowerShell. This is an alternative method for if you want to deploy FortiGate-VM on instance types/sizes that are not found on the FortiGate marketplace launcher. Some instance types of your choice may not properly boot up or run due to lack of official FortiGate instance support.

You can also specify bootstrapping FortiGate CLI commands as art of a bootstrapping configuration file that is passed in PowerShell at the time of initial bootup.

That you have thorough knowledge of PowerShell and various Azure services and features to adopt this deployment method is expected.

Running PowerShell to deploy FortiGate-VM

The instructions assume that PowerShell is already installed on the Windows machine. For details on installing and running PowerShell, see Install Azure PowerShell on Windows with PowerShellGet.

To run PowerShell to deploy FortiGate-VM:

1. Log into a Windows machine and invoke the PowerShell console.
2. Obtain the sample PowerShell script file from GitHub.
3. Edit the content according to your own Azure environment. The ps1 file contains comments for sections that require modification. Editing the file using Visual Studio with the PowerShell extension installed is recommended.
   One of the sections you must modify is the `$vmsize` field. Enter the desired instance type based on the number of virtual CPU cores. Recommended types are the following compute-optimized instances:
   - Standard_F1
   - Standard_F2

- Standard_F4
- Standard_F8
- Standard_F1s
- Standard_F2s
- Standard_F4s
- Standard_F8s
- Standard_F16s
- Standard_F2s_v2
- Standard_F4s_v2
- Standard_F8s_v2
- Standard_F16s_v2
- Standard_F32s_v2
- Standard_F64s_v2
- Standard_F72s_v2

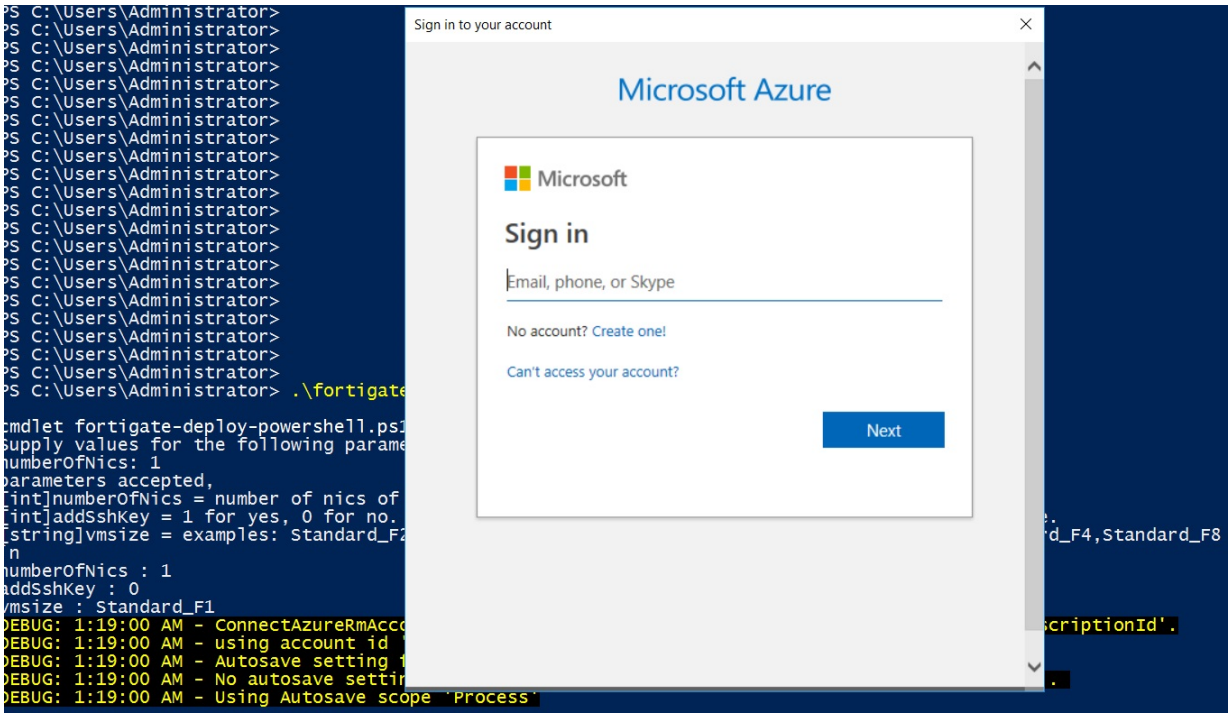
Instances with over 32 vCPU require a FG-VMUL license, which can support an unlimited number of CPU cores.

4. This sample file can deploy the FortiGate-VM in an existing VNet under an existing resource group. Before running the ps1 file, you must create the following Azure elements:
   a. Resource group
   b. VNet with a subnet. If you attach more than one NIC to the FortiGate-VM, create as many subnets as the number of NICs before running the ps1 file.
   c. Container to copy your FortiGate-VM image file
   d. Blob where to create an OS and a data disk file to launch a FortiGate-VM instance
5. You must manually create security groups and route tables after deploying the FortiGate-VM, as the sample ps1 file does not create these.
6. Download the FortiGate-VM vhd image:
   a. Go to Customer Service & Support > Download > VM Images.
   b. From the *Select Product* dropdown list, select *FortiGate*.
   c. From the *Select Platform* dropdown list, select *Azure*.
   d. Download the *FGT_ARM64_AZURE-v7.6.X.F-buildXXXX-FORTINET.out.hyperv.zip* file.
   e. Unzip the downloaded file. Place the *fortios.vhd* file in the *C:\Azure\vhds* directory. You can change the path using the `$sourceVhd` parameter in the ps1 file.
7. Run the ps1 file. In this example, the filename is *fortigate-deploy-powershell.ps1*.

```
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> .\fortigate-deploy-powershell.ps1
```

a. The system prompts you for a number of network instances. Enter a number between 1 and 4.

b. The system prompts you to log into Azure by entering your username and password. Enter your credentials.



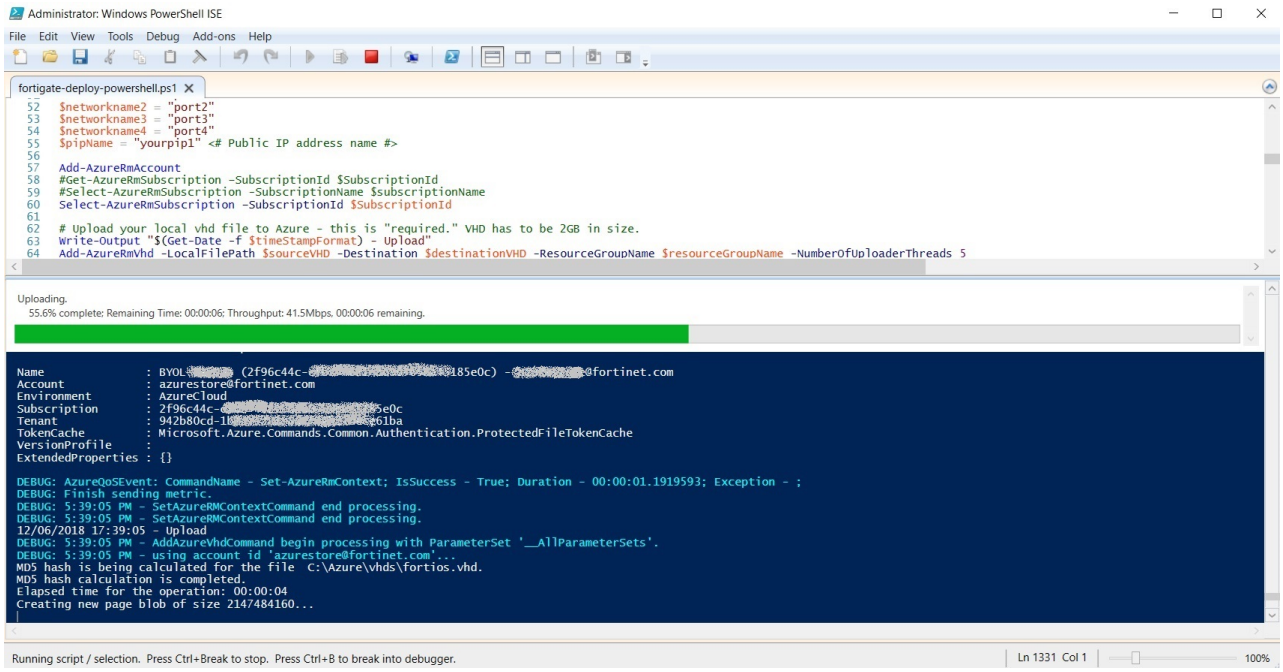
c. The execution continues. If you encounter an error (shown in red), resolve it, manually clean up newly generated files, then retry the execution. If you do not clean up the files, the next execution attempt results in an error. Manually clean up files by doing the following:

i. Remove files created in your container and blob under your storage account.

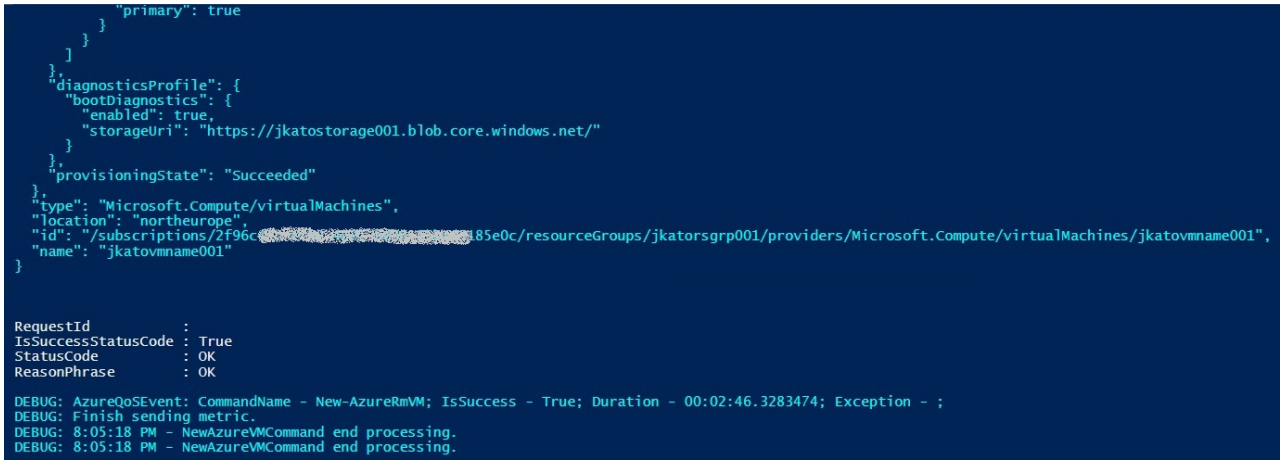
ii. Remove network resources created under your specified resource group.

iii. Diagnostic files are created under your storage account. Remove these files if they are unnecessary.

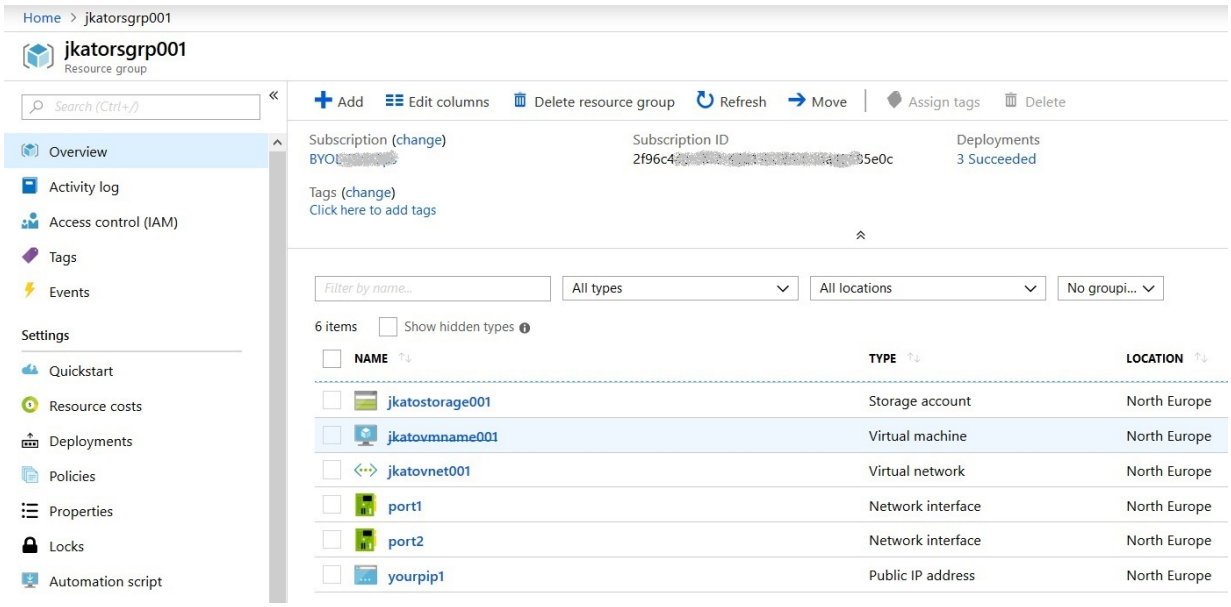
The sample ps1 file is provided for your reference. If you need to modify or author it as required by your organization, you are expected to be able to do so on your own.



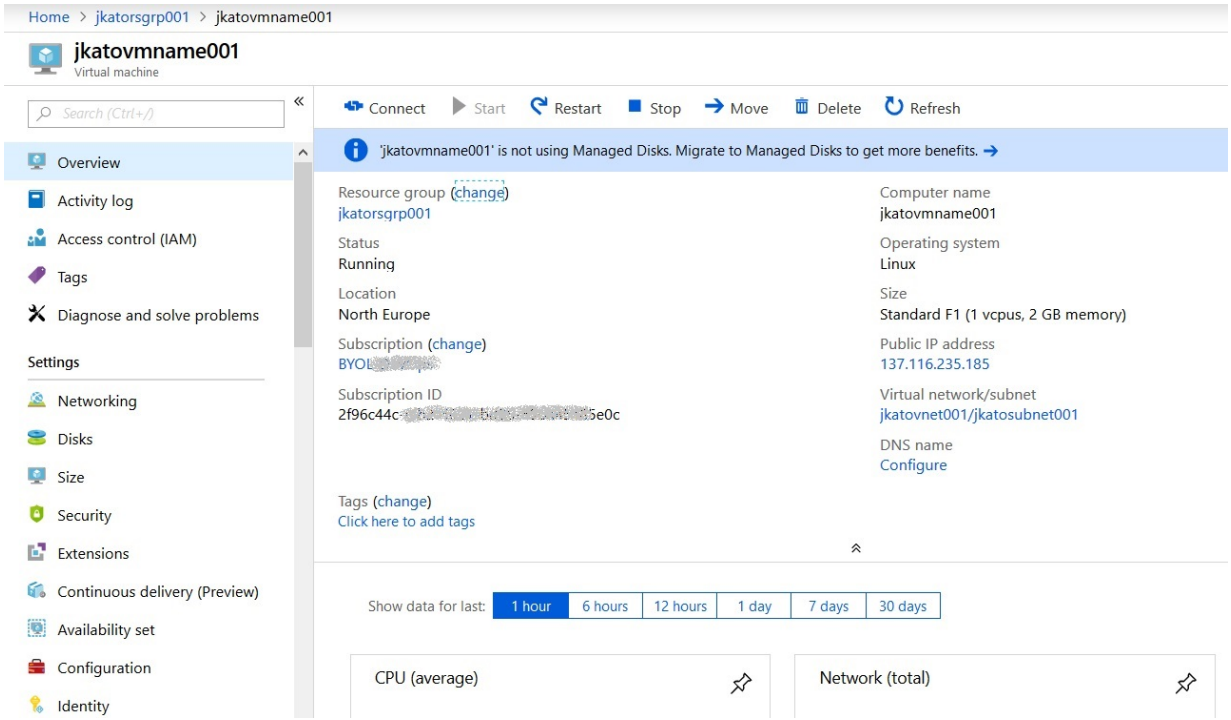
Execution takes about ten minutes to complete.



8. Access the FortiGate-VM after executing the ps1 file:
   a. Navigate to the resource group and click the specified VM name.

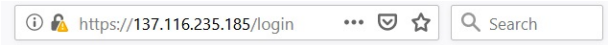


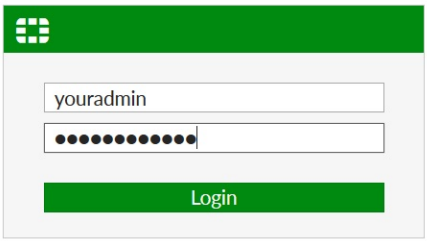
   b. Click the FortiGate-VM hostname and find its public IP address.



   c. In a browser, access https://<public IP address>. Enter the admin username and password specified in the ps1

file to log in.





Bootstrapping the FortiGate CLI and BYOL license at initial bootup using user data

This section explains how to add bootstrapping of FortiGate CLI commands and BYOL license at the time of initial bootup as part of PowerShell deployment.

It is expected that you have thorough knowledge of PowerShell and various Azure services and features to adopt this deployment method. You should be able to author a ps1 file on your own as required by your organization.

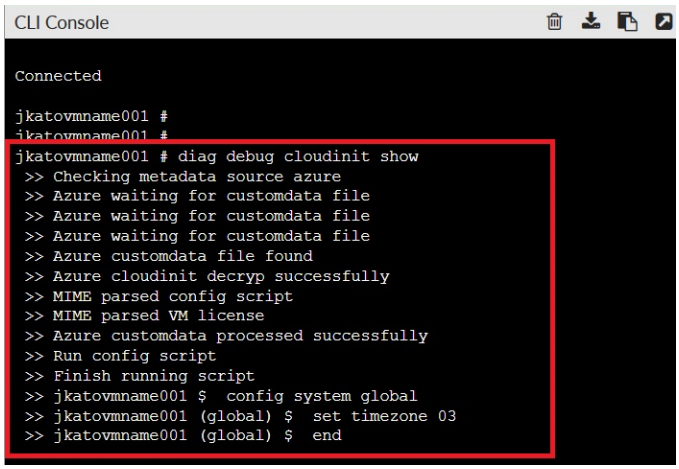
You can find a sample PowerShell script that works with bootstrapping on GitHub.

To bootstrap the FortiOS CLI and BYOL license at initial bootup using user data:

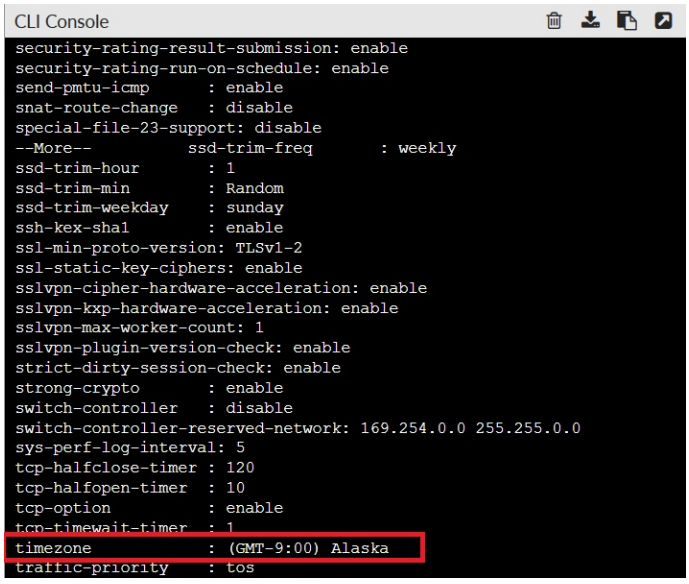
1. Create a directory on your PC with the path C:\Azure\misc.
2. Create a MIME text file named azureinit.conf in the C:\Azure\misc directory. You can change the directory path and file name using the `$customdataFile = C:\Azure\misc\azureinit.conf` parameter in the ps1 file. azureinit.conf is the text file in MIME format that includes both FortiGate CLI commands and license file content. You can download a sample azureinit.conf from GitHub.
3. You can download a license file from Customer Service & Support after registering your product code. Copy and paste the content of your license file to replace the license portion of azureinit.conf. FortiGate-VM license content resembles the following:

```
-----BEGIN FGT VM LICENSE-----
QAAAABUiZtrwrJdUjEe/8C5dNVnOvmY1w7OZWXPPTG7vm2KKwYvL4++qL0gED6/q
SQSPkwpTFlXjAuRGtGyX1VvaTpXgGQAA1pwrFdJnS6TWJ6dVT7KiD8ncufaa3bCw
s8XpmLivzjE4//+C9nqh4fN/KyDweWEIptDMaNsoCm0B0rU8HQIDkX+rgeCs3QZ5
ELStRrXil/oXqTB/gorG67ZdybxWvzPWvWJYDS5AsI+QK8BHJ+xGhLjhkzBZ4ezU
Hd01HCSm7MXEYV5KauU43sZ9XEStxqPEInah3yXgYTd24pnV683G4EHCkAdGyMTP
QqDqBMKcT5aei0ooGVAOX8D62C5Zjh+r1+tkdpR5YHoVYZHU95hBCNjBroJbMnK7
NogYuadQEh28MDtpvzXnb24mW1fDQMTJysQwCtwzJzmnBnvSBo7xNq/irTs2QnFB
O3pizyJ7rMJguXpCB/3v018qAXoqbL5Ks7aQHQTqNuRL2SMducwfd1iAbfz7TMN9
bnbRMz3n5VJUiP+eIFiV84yfwOcCJl+NZAP0hqL3DGBt4urwRFV6yndVi3wZG6hn
eV4LIHkJ5T25/b14m9I+fqEXEsSKKKPn7H2wdyroBdw+VLnT9Hk+3H7t3IL29AZ+
+FDMeRM+BooWnHG3y5do6DB+Wi+CIuxqmNIaoln9buNyFH5bcGU92/6APuFFQ8dI
3DNLIc6ZKDpq7j2ti79dHoIYxCG0S8UsC6l3lOsSwjHg+rO6x+YAEtP0//ktuIvh
NeAFiJveJRxbZBJAu1qnjzNc9Wt7Rg9LvDnwvVKl6Afop2Kt+icfxRL1gySqhWdo
b56XyJbIqAwb/JLa6EkmZDrn3sWQ4H9K
-----END FGT VM LICENSE-----
```

4. In the example ps1 file, the FortiGate CLI command is shown as the following:
   ```
   config system global
   set timezone 03
   end
   ```
   This example sets the timezone as GMT-9 Alaska. You can replace these lines with your own set of CLI commands.
5. After editing the sample ps1 file to reflect your own Azure environments and azureinit.conf file as required, run the ps1 file. It reads the conf file and passes FortiGate CLI commands and the license to the FortiGate-VM deployment using cloud-init user data.
6. After the ps1 file execution ends, log into the FortiGate by accessing *https://<IP_address>* in your browser.
7. The system displays the dashboard instead of a license upload window, since the license is already activated.
   To see how bootstrapping went, check if the command was successfully run. Open the CLI console and enter `diag debug cloudinit show`.
   If the cloud-init was run successfully, the CLI shows `Azure customdata processed successfully`.



   If you see an error with this `diagnose` command, resolve it and try again by editing azureinit.conf. There may be a syntax error.
8. Check the timezone by running `config system global` and `get` commands.



   The timezone was changed to Alaska as expected, meaning that the bootstrapping CLI command was successful. This assumes that you used the default FortiGate CLI command in step 4. If you modified the command, test it

accordingly.

Deploying FortiGate-VM on regional Azure clouds

In addition to "global" Azure support, FortiGate-VM supports "regional" Azure support, including China, Germany, and U.S. Gov. FortiGate-VM deployment on regional Azure clouds requires dedicated subscription accounts as they are not covered by global Azure and services are run under URL domains unique to the regional Azure cloud.

FortiGate-VM is not available on regional Azure cloud marketplaces. Instead, you can deploy FortiGate-VM (BYOL) having a VHD file ready and instantiating a FortiGate-VM instance using your PowerShell or ARM deployment templates by pointing to the VHD file.

You can download the VHD file from Fortinet Customer Service & Support. Go to *Download* > *VM Image*, then select *FortiGate* as the *Product* and *Azure* for the *Platform*. The file name is FGT_VM64_AZURE-v6-buildXXXX-FORTINET.out.hyperv.zip, where XXXX is the build number.

Once the download is complete, unzip the file and locate the fortios.vhd file. Upload the fortios.vhd file to your blob/storage location as required by your deployment templates.

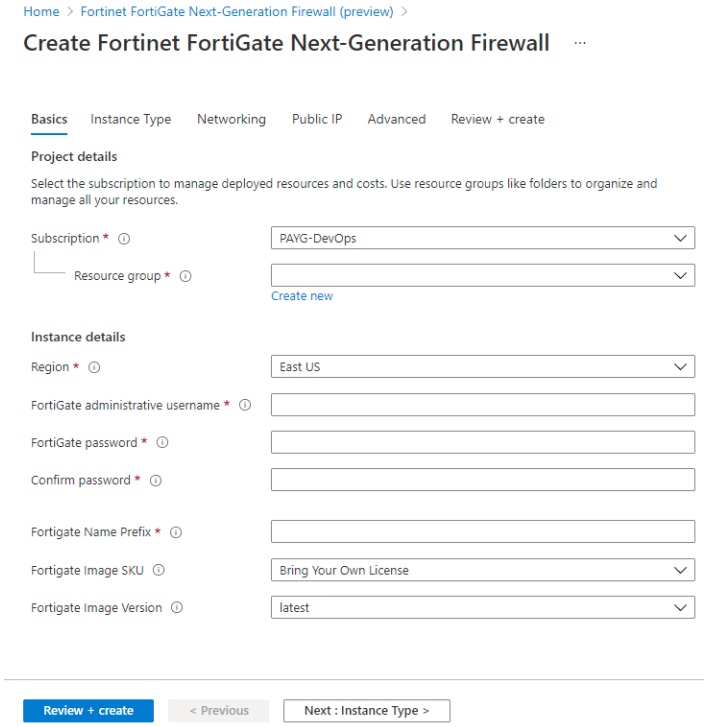
Deploying FortiGate-VM from the marketplace

To deploy FortiGate-VM from the marketplace:

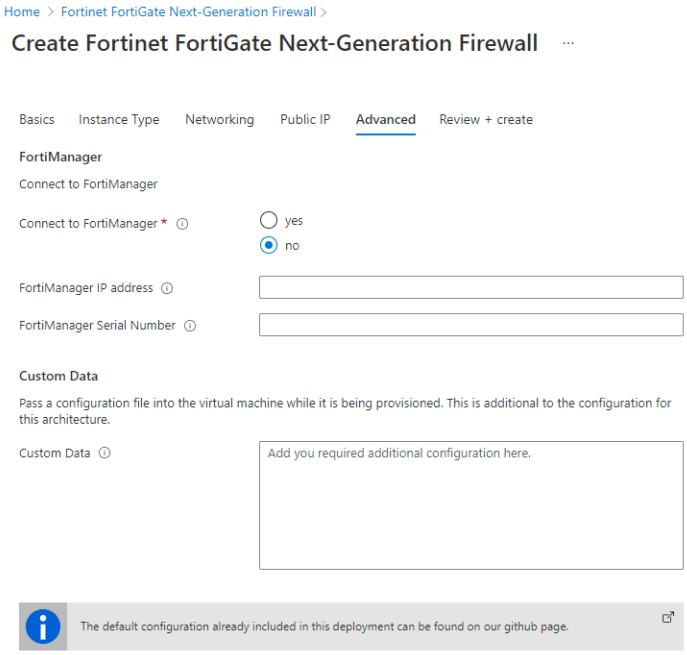
1. In the Azure marketplace, search for and select Fortinet FortiGate Next-Generation Firewall. Ensure that the listing says *Azure Application*.

2. From *Select a plan*, select the desired deployment plan. Click *Create*.
3. On the *Basics* tab, configure the parameters according to your requirements:
   a. From the *Subscription* dropdown list, select your subscription.
   b. In *Resource group*, select an existing resource group or create a new one.

c. From the *Region* dropdown list, select the desired region.
d. In the *FortiGate administrative username* and *password* fields, enter the username and password for the FortiGate administrative profile.
e. In the *FortiGate Name Prefix* field, assign a naming prefix for your FortiGate resources.
f. From the *FortiGate Image SKU* dropdown list, select bring your own license (BYOL) or pay as you go (PAYG).
g. From the *FortiGate Image Version* dropdown list, select the FortiGate version to deploy.
h. Click *Next: Instance Type >*.



4. On the *Instance Type* tab, select an appropriately sized instance type. Click *Next: Networking >*.
5. On the *Networking* tab, configure the parameters according to your requirements:
   a. In *Virtual network*, select an existing VNet or create a new one. The FortiGate-VM requires a public and private interface for internet edge protection.
   b. Enable or disable *Accelerated Networking*, which refers to SR-IOV support. This depends on the instance type that you selected.
   c. Click *Next: Public IP >*.
6. On the *Public IP* tab, create a new public IP address or create a new one. Click *Next: Advanced >*.
7. On the *Advanced* tab, configure the parameters according to your requirements:
   a. If you want FortiManager to manage this FortiGate, enable *Connect to FortiManager* and provide the FortiManager IP address and serial number in the *FortiManager IP address* and *FortiManager Serial Number* fields.
   b. To provide initial configuration to the FortiGate, enter the desired commands in the *Custom Data* field. Azure executes these commands during initial bootup.



c. To provide a BYOL license file for the FortiGate, upload it using the *FortiGate License* field. Azure ignores the license file if you selected PAYG in step 3. Click *Next: Review + create >*.

8. Once validation completes, confirm all values, then click *Create*. Azure creates the resources accordingly.

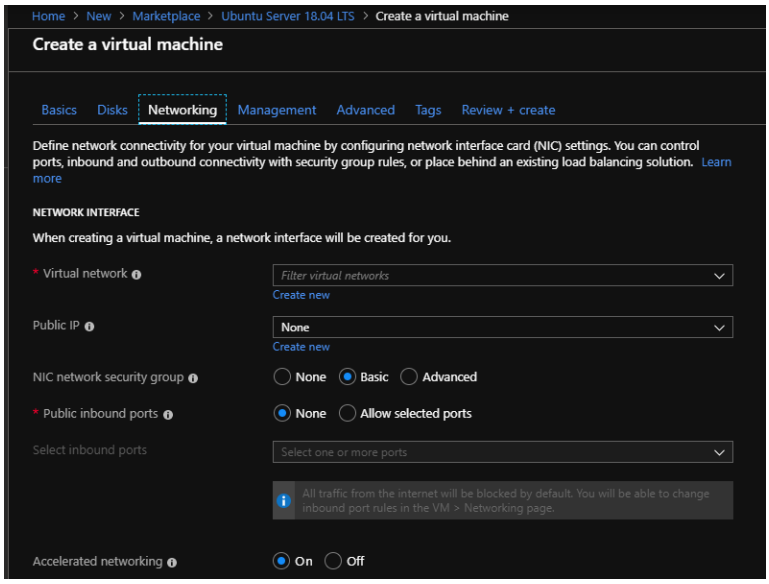
Enabling accelerated networking on the FortiGate-VM

Azure supports SR-IOV, which accelerates networking by allowing VM NICs to bypass the hypervisor and go directly to the PCIe card underneath. FortiOS must understand when it is using SR-IOV and change networking to accommodate SR-IOV.

Azure refers to SR-IOV as *Accelerated Networking*. You can check if it is enabled by checking the NIC attached to the VM through the GUI or CLI.

To configure accelerated networking:

1. You can enable accelerated networking when instantiating a new VM, or enable it after the VM has been created. Do one of the following:
   - To enable accelerated networking using the GUI, create a new VM or select an existing VM. On the *Networking* tab, for *Accelerated networking*, select *On*.



- To enable accelerated networking using the CLI, run the following commands:

```
root@mail:/home/azure/images# az network nic update -g <Resource group name> -n <NIC
     name> --accelerated-networking true
{
"dnsSettings": {
"appliedDnsServers": [],
"dnsServers": [],
"internalDnsNameLabel": null,
"internalDomainNameSuffix": "k41kcrl04yeezbyeswqimbxshb.fx.internal.cloudapp.net",
"internalFqdn": null
},
"enableAcceleratedNetworking": true,
```

On the FortiOS side, a virtual interface is created in the format of sriovslv(number) for each NIC that has accelerated networking enabled:

```
<VM name> # fnsysctl ifconfig
port1 Link encap:Ethernet HWaddr 00:0D:3A:B4:87:70
   inet addr:172.29.0.4 Bcast:172.29.0.255 Mask:255.255.255.0
   UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
   RX packets:5689 errors:0 dropped:0 overruns:0 frame:0
   TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
   collisions:0 txqueuelen:1000
   RX bytes:1548978 (1.5 MB) TX bytes:0 (0 Bytes)
sriovslv0 Link encap:Ethernet HWaddr 00:0D:3A:B4:87:70
   UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
   RX packets:35007 errors:0 dropped:0 overruns:0 frame:0
   TX packets:33674 errors:0 dropped:0 overruns:0 carrier:0
   collisions:0 txqueuelen:1000
   RX bytes:34705194 (33.1 MB) TX bytes:10303956 (9.8 MB)
```

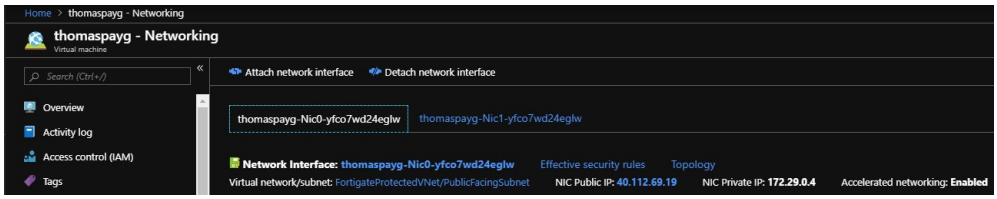
The NIC shows the driver as `hv_netvsc` with accelerated networking enabled or disabled:

```
<VM name> # diagnose hardware deviceinfo nic port1
Name: port1
Driver: hv_netvsc
```

The FortiOS GUI does not display the virtual interface in *Network* > *Interfaces*.

To check if accelerated networking is enabled using the GUI:

1. In the Azure management console, go to the desired VM, then *Networking*.
2. Select the desired NIC. In this example, accelerated networking is shown as enabled.



To check if accelerated networking is enabled using the CLI:

```
root@mail:/home/azure/images# az network nic show -g <Resource group name> -n <NIC name>
```

Check that the following displays as part of the output: `"enableAcceleratedNetworking": true,`

Upgrading FortiOS

For the recommended upgrade path, see Upgrade Path Tool. For pay as you go, select *FortiGate-VM-AZUREONDEMAND*. For bring your own license, select *FortiGate-VM-AZURE*. Select the current and target upgrade versions to see the upgrade path.

Deploying autoscaling on Azure

You can deploy FortiGate virtual machines (VMs) to support autoscaling on Azure. New resources are created or existing resources are used when specified during the deployment. By integrating FortiAnalyzer, you can consolidate logging and reporting for your FortiGate cluster. Fortinet provides a FortiGate Autoscale for Azure deployment package to facilitate the deployment.

Multiple FortiGate-VM instances form Virtual Machine Scale Sets (VMSS) to provide highly efficient clustering at times of high workloads. FortiGate Autoscale for Azure incorporates one or more VMSS, network related components, and Azure Function App scripts. FortiGate-VM instances are scaled out automatically according to predefined workload levels. When a spike in traffic occurs, FortiGate-VM instances are automatically added to the VMSS. Autoscaling is achieved by using FortiGate-native high availability (HA) features such as `config-sync`, which synchronizes operating system (OS) configurations across multiple FortiGate-VM instances at the time of scale-out events.

FortiGate Autoscale for Azure is available with FortiOS 6.4.5, FortiOS 6.4.7, FortiOS 7.0.0, and FortiOS 7.0.1 and supports any combination of On-Demand (PAYG) and Bring Your Own License (BYOL) instances.

FortiAnalyzer 6.2.5 or FortiAnalyzer 6.4.5 can be incorporated into Fortinet FortiGate Autoscale to use extended features that include storing logs into FortiAnalyzer.

Overview

The virtual network

The virtual network (VNet) requires at least one subnet, referred as *Subnet 1*. Other subnets are optional.

- The required subnet is directly associated with FortiGate Autoscale.
- Two FortiGate VMSS will be deployed into *Subnet 1*.
- *Subnet 1* will be associated with *Port 1* on the FortiGate.
- One Network Security Group is be associated with *Subnet 1*.

The FortiGate Autoscale deployment template can configure up to 4 subnets per FortiGate in the cluster.

- Each FortiGate will initially have one Network Interface available per subnet.
- Additional subnets specified in the template will be associated as Port 2, Port 3, and Port 4 (as required) on the FortiGate. The association of ports depends on the order in which the subnet is specified in the template.
  - In a 3-subnet deployment, Port 2 will point to the subnet with the lower number and Port 3 will point to the subnet with the higher number. Port 4 will not be used.
  - In a 2-subnet deployment, Port 2 will point to the subnet. Ports 3 and 4 will not be used.

- Example scenarios are described in the table below.

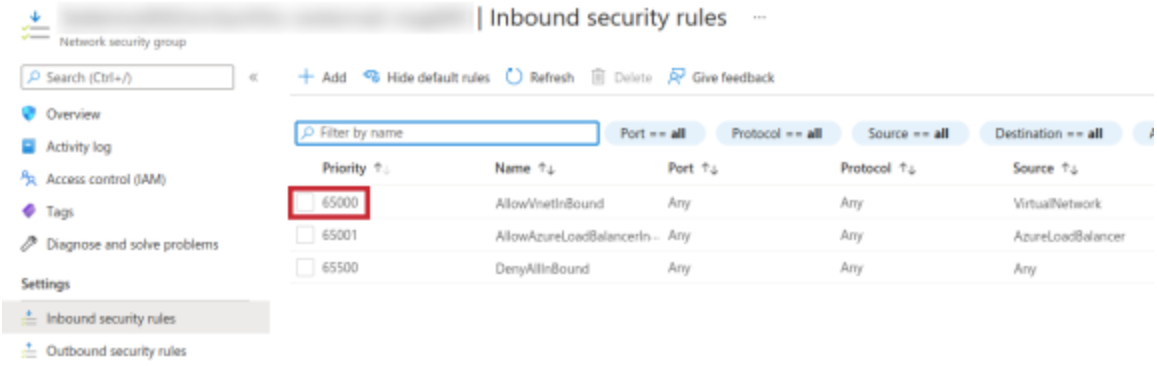
Scenario	Subnet parameter on the template	FortiGate port associations
4-subnet deployment	Subnet 2: ✓ Subnet 3: ✓ Subnet 4: ✓	Port 2 points to Subnet 2. Port 3 points to Subnet 3. Port 4 points to Subnet 4.
3-subnet deployment	Subnet 2: ✓ Subnet 3: ✕ Subnet 4: ✓	Port 2 points to Subnet 2. Port 3 points to Subnet 4.
2-subnet deployment	Subnet 2: ✕ Subnet 3: ✕ Subnet 4: ✓	 Port 2 points to Subnet 4.

- FortiGate Autoscale will be only configured for the subnets specified in the virtual network.
  - Users can modify the virtual network after the initial deployment. In this case, additional manual configuration will be required.
- In a multiple subnet deployment scenario, it is recommended that users use one Network Security Group for *Subnet 1*, and another Network Security Group for the other subnets.

The Autoscale resource group must be created in the same region as the VNet resource group specified in the parameter VNet Resource Group Name on page 72.

Subnet 1 Network Security Group Rule Priority

This parameter refers to the highlighted area of the following image:



When using an existing VNet that has associated a network security group with *Subnet 1* (the subnet that will be used to deploy the Autoscale VMSS) the network security group may already have existing rules. As the template deployment will add new rules to this network security group, specifying the *Subnet 1 Network Security Group Rule Priority* parameter can help users avoid potential rule conflicts. For details on setting the rule priority, refer to the Microsoft article Network security groups > Security rules.

FortiAnalyzer integration

When FortiAnalyzer integration is selected, a new FortiAnalyzer resource will be created in the virtual network to be used by FortiGate Autoscale. As FortiGate Autoscale and the FortiAnalyzer are configured to work with each other, this FortiAnalyzer is not intended to be replaced.

FortiAnalyzer requires a public IP address resource to work with and the deployment defaults to creating a new resource.

Using an existing public IP address

By default, the deployment template will create a new public IP address for the FortiAnalyzer (if deploying with FortiAnalyzer integration) and the front-end load balancer. Specifying the ID of a public IP resource will associate the existing resource for use in the FortiGate Autoscale deployment.

To use an existing public IP address:

1. Ensure the public IP address is available for use.
2. Look up the *Resource ID* of the existing public IP resource. This is found in the Properties of the Azure resource.
3. Specify the full *Resource ID* in the relevant parameter:
   - For the FortiAnalyzer, specify the Resource ID in the parameter FortiAnalyzer Public IP Address ID on page 68.
   - For the Front End Load Balancer, specify the Resource ID in the parameter Frontend IP Address ID on page 68.

Confirm the public IP resource quota before starting a deployment to ensure resource allocation is successful. Not enough IP address resources will result in deployment failures.

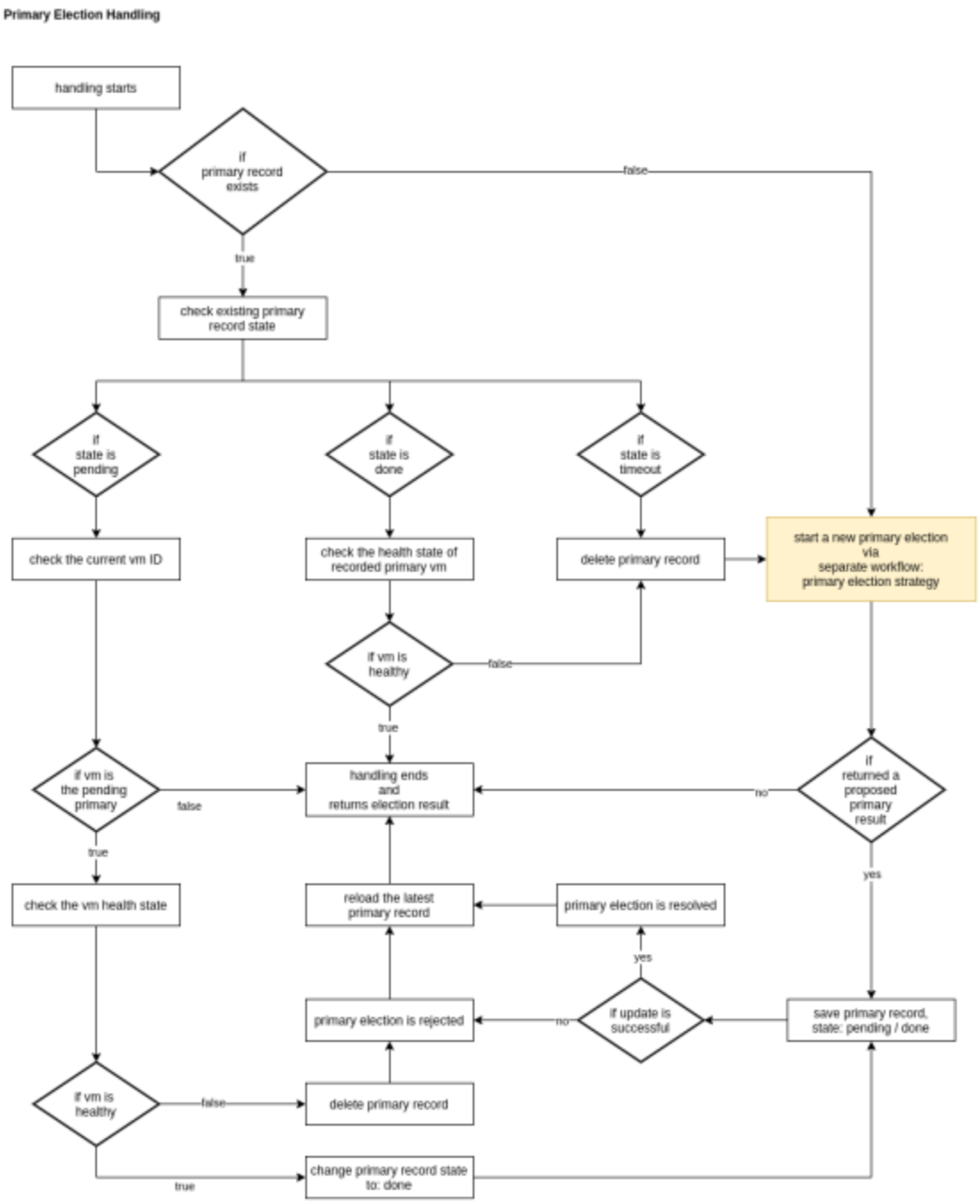
The SKU of the public IP address for the FortiAnalyzer isn't restricted. In comparison, the IP address for the external Load Balancer must be of the 'standard' SKU in order to match the VMSS.

Election of the primary instance

A core feature of FortiGate Autoscale is the election of the primary instance. FortiGates in the VMSS are constantly monitored and if the conditions of the environment have changed, the election of a new primary instance may be required.

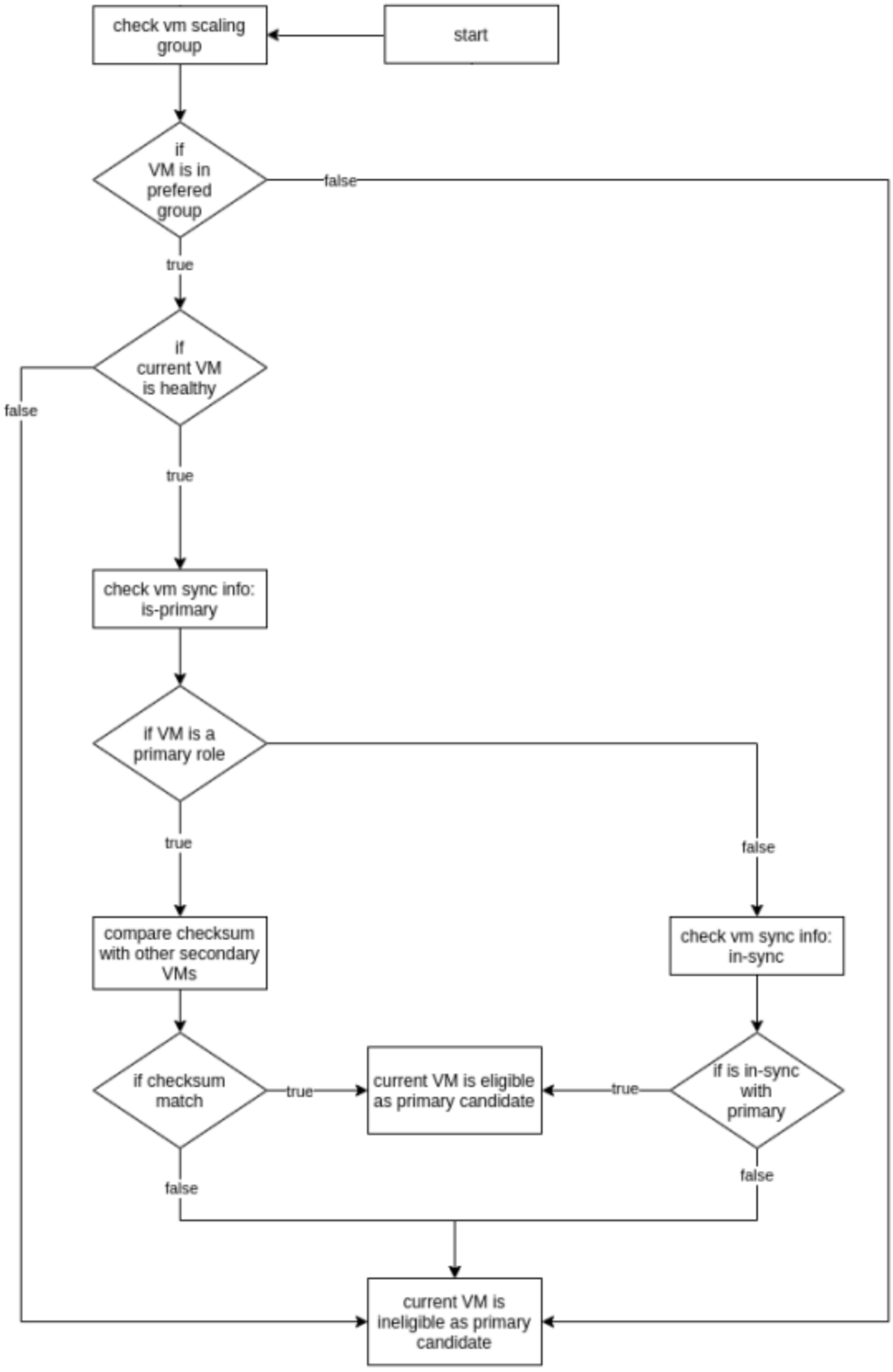
As depicted in the flowchart below, a primary election will happen:

- when no primary record is found in the database
- when the FortiGate noted in the primary record is deemed unhealthy



The preferred group primary election strategy is depicted in the flowchart below:

Flow: Preferred Group Primary Election strategy



Heartbeat

FortiGate Autoscale monitors the heartbeat sent from each FortiGate. The default heartbeat interval is 30 seconds, as defined by the parameter Heart Beat Interval on page 68.

To change the heartbeat interval after deployment:

1. Locate the Settings item with key: *heartbeat-interval*. For details, refer to the section Modifying the Autoscale settings in Cosmos DB on page 82.
2. Update the numeric value to the desired duration.
3. Update the `auto-scale hb-interval` interval on the primary FortiGate to match the value specified in the Cosmos DB using the following:
```
config system auto-scale
set hb-interval <desired interval>
end
```

Late heartbeat

The FortiGate sends heartbeats to the Autoscale handler via HTTPS. As such, network conditions may result in heartbeats arriving later than expected. When this happens, the heartbeat is considered a late heartbeat and the Heart Beat Loss Count on page 68 will be increased by 1.

Heartbeat loss count

Any late heartbeat will increase the heartbeat loss count by 1. If this count reaches a defined threshold, the FortiGate will be deemed temporarily unhealthy. Any heartbeat arriving at the handler on time will reset the count to 0. The default heartbeat loss count is 10 (seconds) and is defined in the parameter Heart Beat Loss Count on page 68.

To change the heartbeat loss count after deployment:

1. Locate the Settings item with key: *heartbeat-loss-count*. For details, refer to the section Modifying the Autoscale settings in Cosmos DB on page 82.
2. Update the numeric value to the desired duration.

Heartbeat delay allowance

FortiGate Autoscale offsets a certain amount of network latency on the Internet with the parameter Heart Beat Delay Allowance on page 68. The default allowance is 2 seconds.

To change the heartbeat delay allowance after deployment:

1. Locate the Settings item with key: *heartbeat-delay-allowance*. For details, refer to the section Modifying the Autoscale settings in Cosmos DB on page 82.
2. Update the numeric value to the desired duration.

Unhealthy state and eligibility for primary role

A FortiGate-VM in an unhealthy state is excluded from participating in the election of the primary instance.

If the current primary FortiGate is deemed unhealthy, it will still work in the primary role until the next Primary Election, after which the primary role will be assigned to another eligible FortiGate and the previous primary FortiGate will change its role to secondary during its next heartbeat.

An unhealthy VM will stay running in the cluster in a secondary role until it recovers from the unhealthy state. This behavior does not cause any scaling activity to happen.

It takes some time, usually within one heartbeat interval, for each FortiGate to be individually notified about the new primary so the change of primary does not happen synchronously on every FortiGate but eventually they will be in-sync with the new primary.

Sync recovery count

FortiGate Autoscale helps an unhealthy FortiGate recover by counting the on-time heartbeats it sends. When the counter reaches the sync recovery count, the FortiGate is deemed healthy and is again eligible to be elected the primary instance.

To change the sync recovery count after deployment:

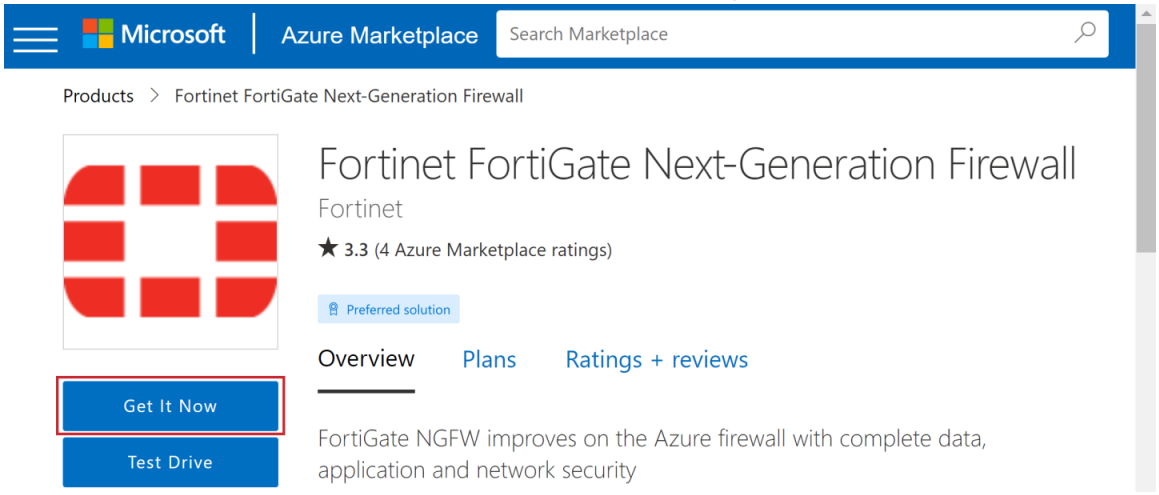
1. Locate the Settings item with key: *sync-recovery*. For details, refer to the section Modifying the Autoscale settings in Cosmos DB on page 82.
2. Update the numeric value to the desired duration.

Selecting the instance type

The size of the FortiGate and the size of the FortiAnalyzer (optional) are specified in the Instance Type on page 68 and FortiAnalyzer Instance Type on page 67 parameters. The string value entered in these parameters is created from the words of the size.

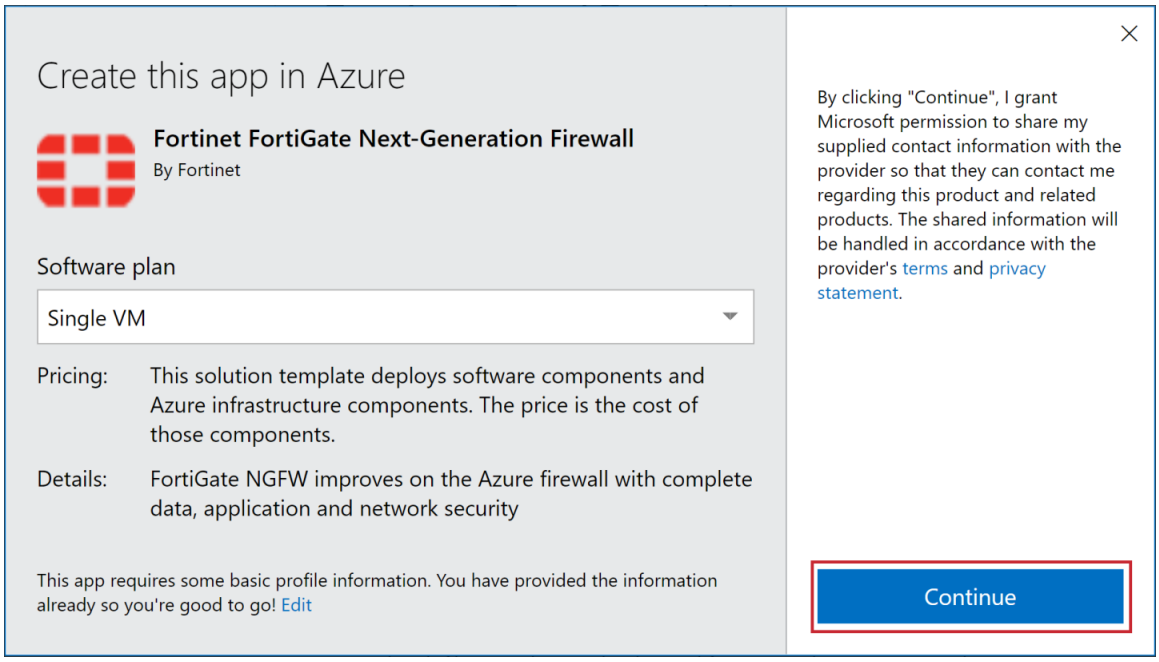
To select the instance type for FortiGate:

1. Go to Fortinet FortiGate Next-Generation Firewall in Azure Marketplace.

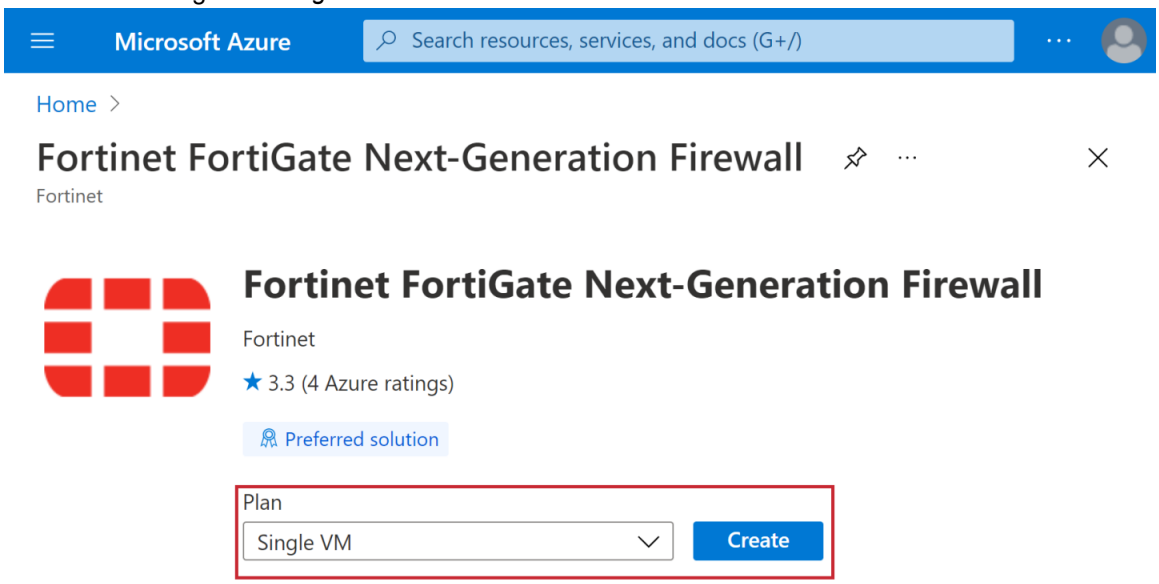


2. Click *Get It Now*.

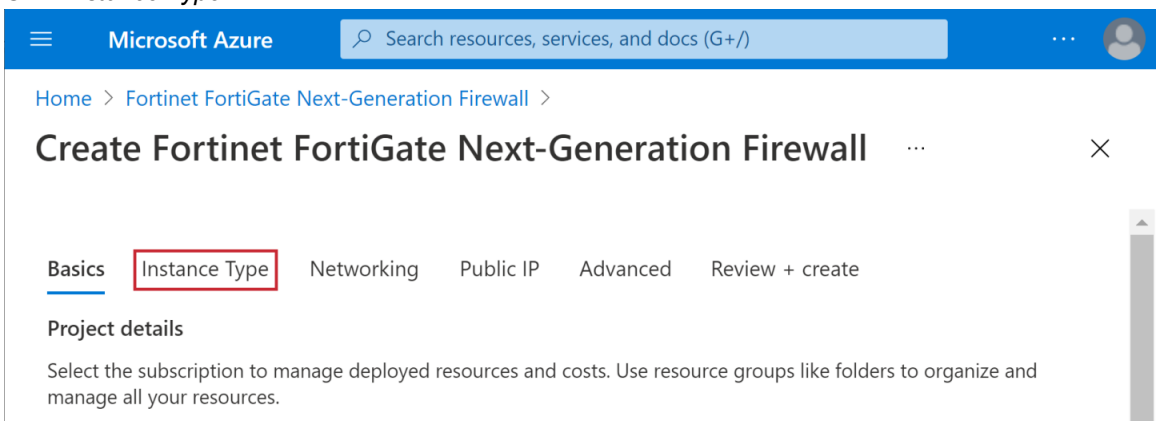
3. Click *Continue*.



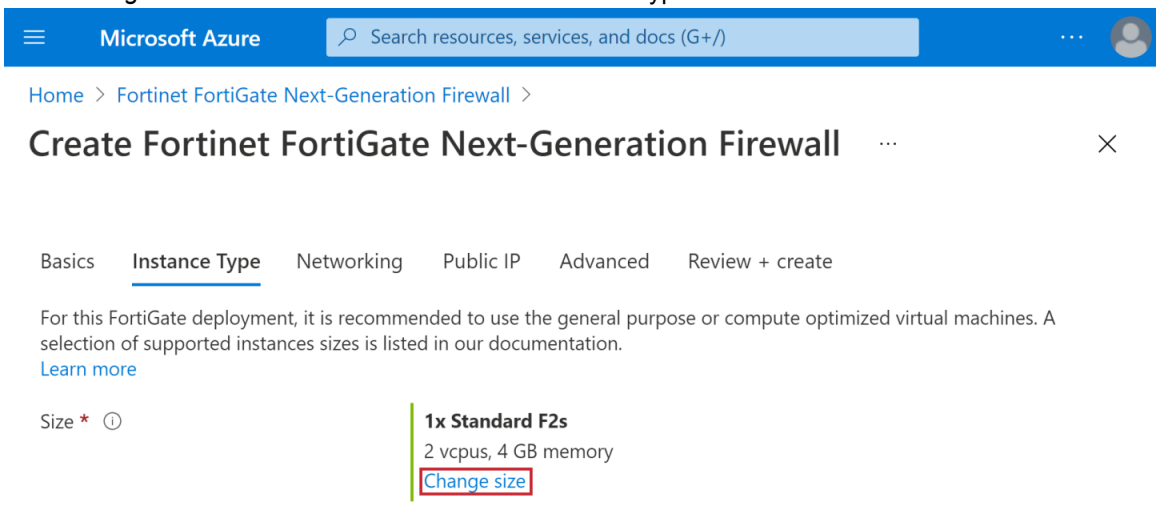
4. Click *Create* using *Plan: Single VM*.



5. Click *Instance Type* as illustrated.



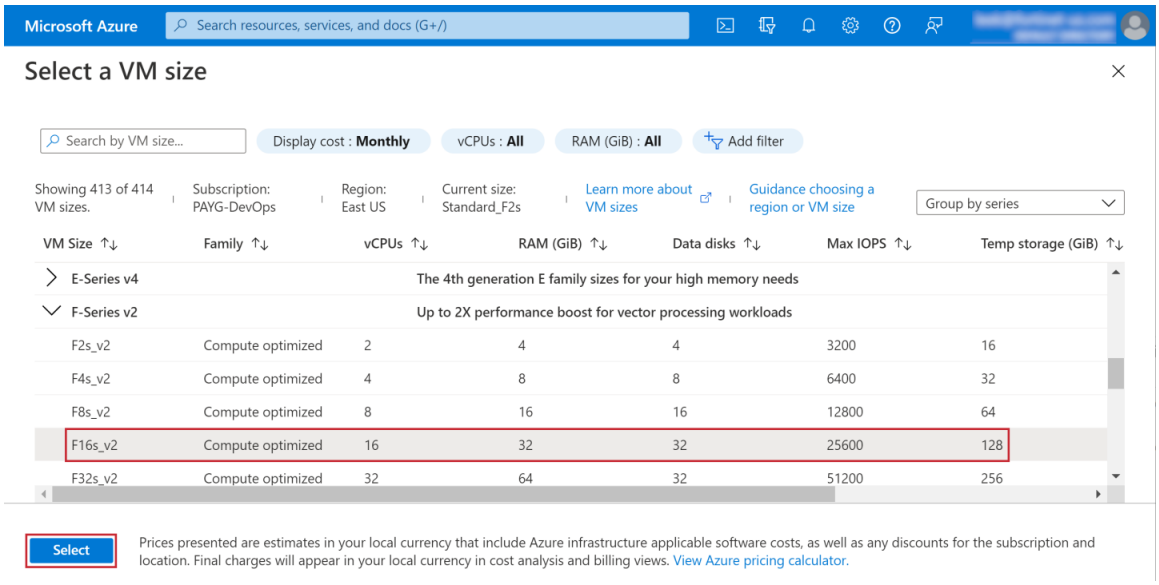
6. Click *Change size* to view the full list of available Instance types.



7. Review the information and capacity of the VM sizes and select the best one for your deployment.

For BYOL VM sizes, users should also match the vCPU capacity of the selected *Instance Type* with the limit of the FortiGate license. Each license has a limit for the maximum number of vCPU per VM.

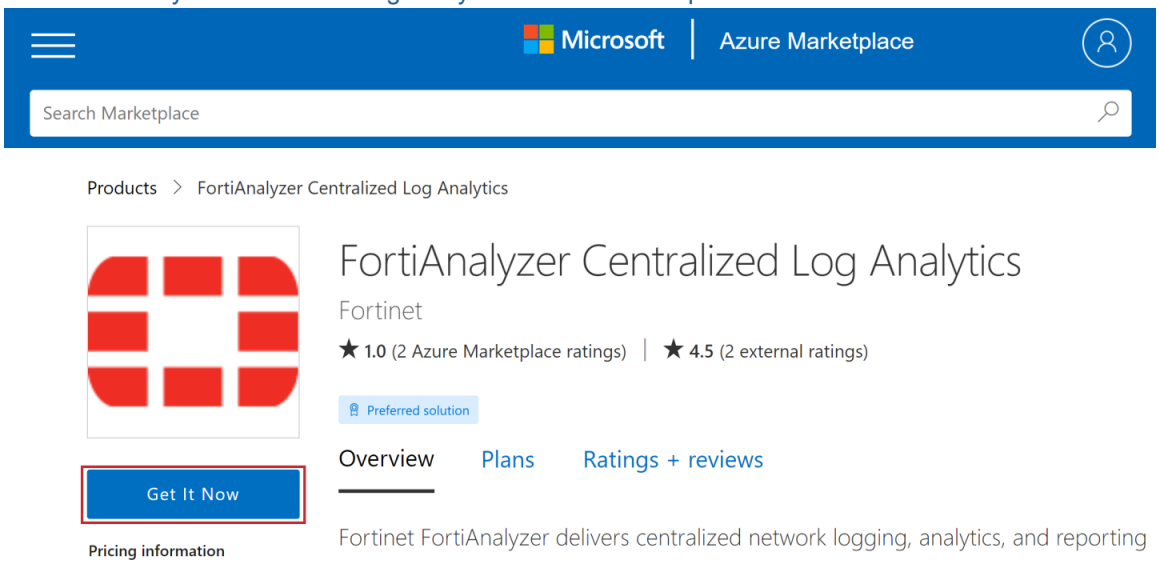
In the example below, *F16s_v2* is chosen.



8. Click *Select*.

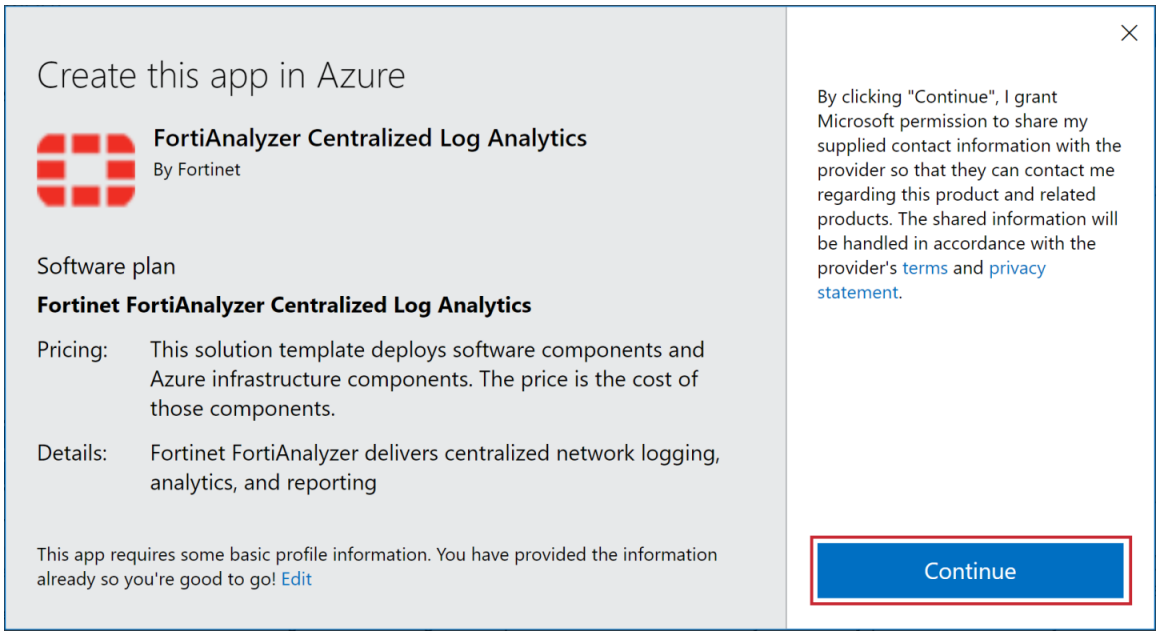
To select the instance type for FortiAnalyzer:

1. Go to FortiAnalyzer Centralized Log Analytics in Azure Marketplace.

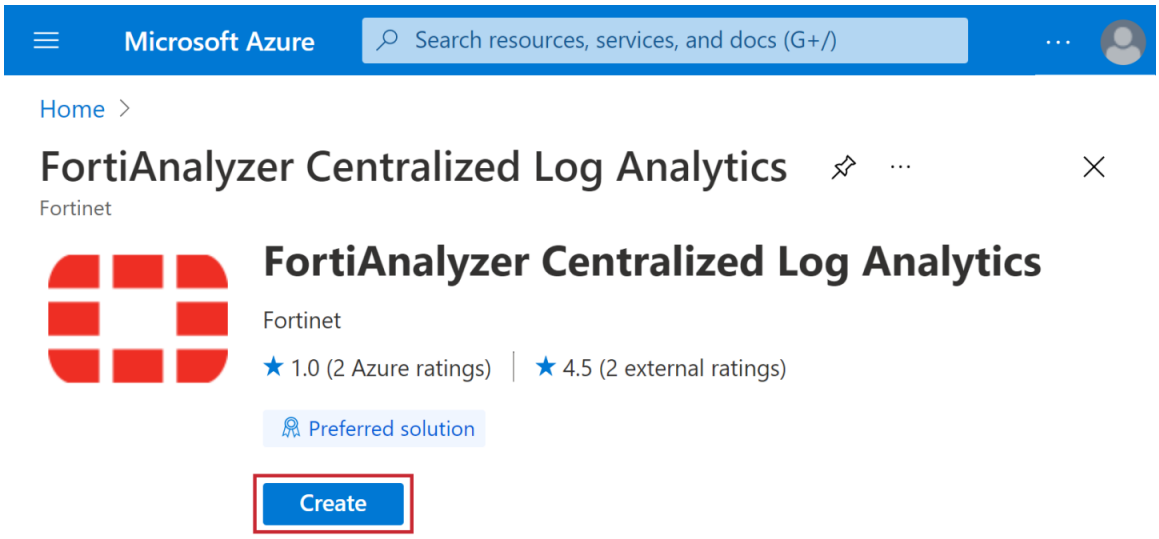


2. Click *Get It Now*.

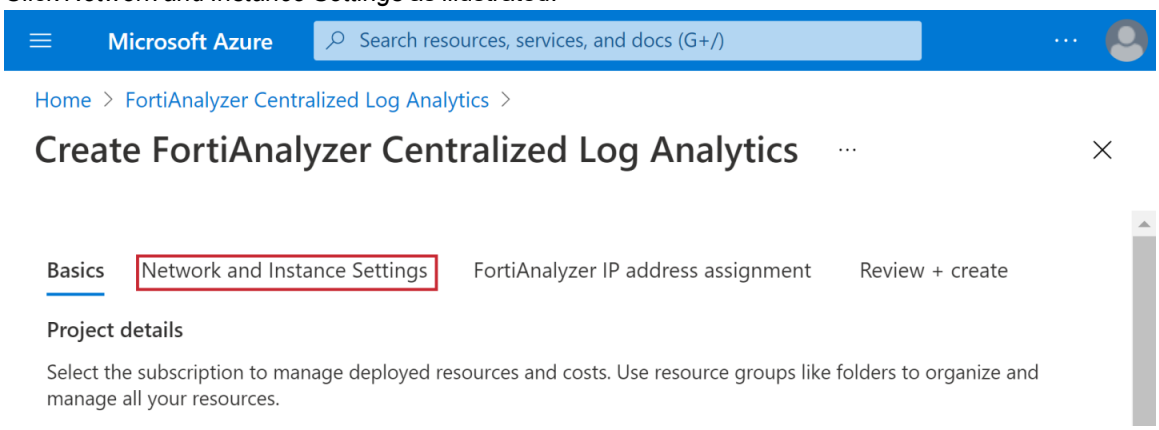
3. Click *Continue*.



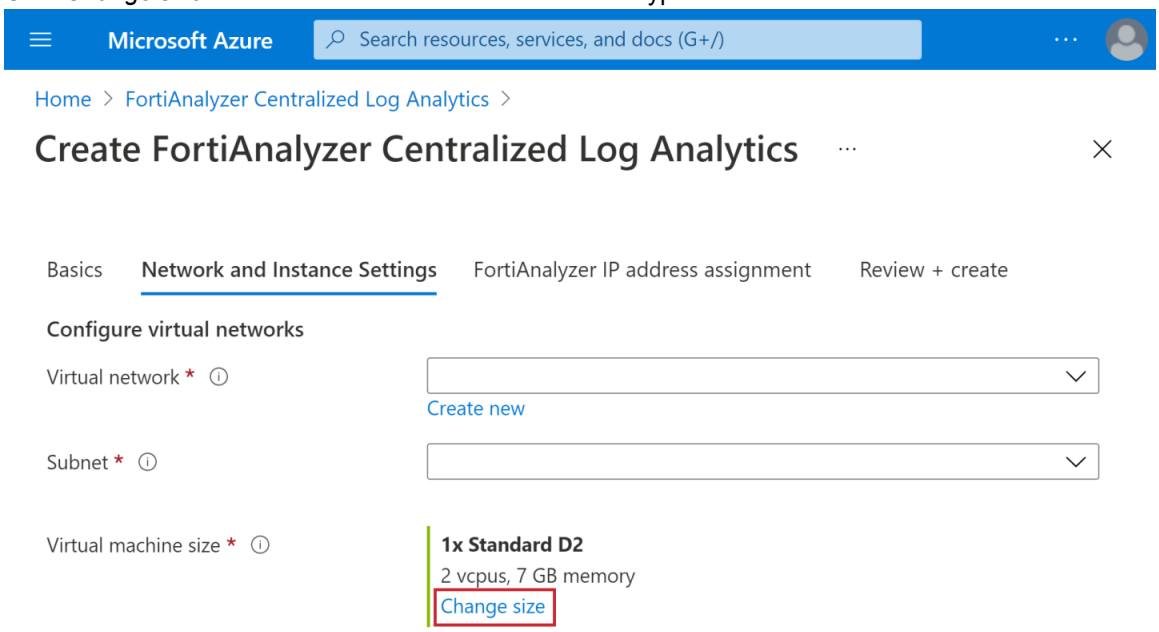
4. Click *Create*.



5. Click *Network and Instance Settings* as illustrated.



6. Click *Change size* to view the full list of available instance types.



7. Review the information and capacity of the VM sizes and select the best one for your deployment.

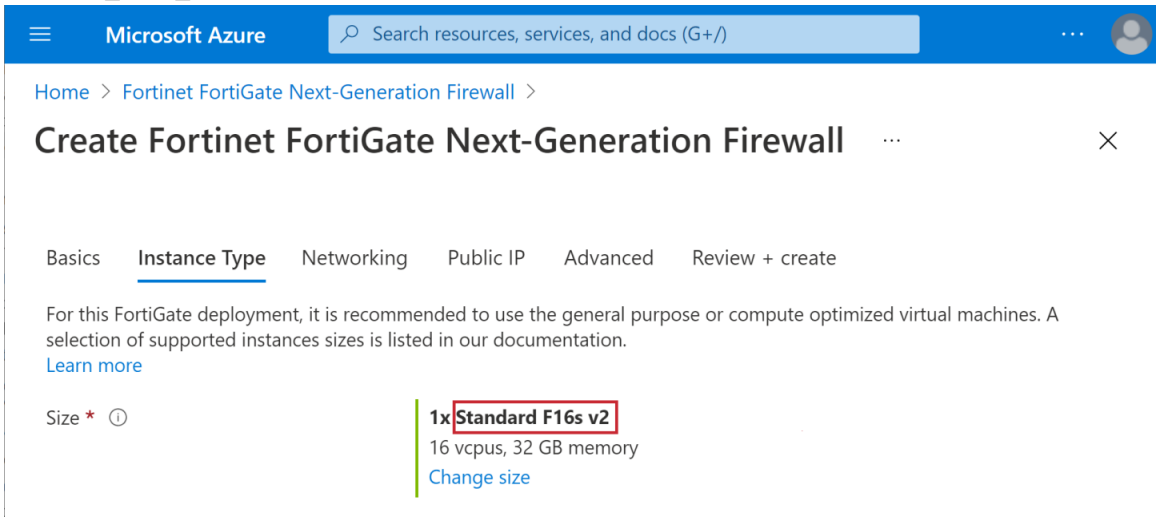
> For BYOL VM sizes, users should also match the vCPU capacity of the selected Instance Type with their FortiGate License. The License has a limit for the maximum number of vCPU per VM.

8. Click *Select*.

To create the instance type string:

During the template deployment the FortiGate instance type is entered in the parameter Instance Type on page 68 and the FortiAnalyzer instance type is entered in the parameter FortiAnalyzer Instance Type on page 67. The value of each instance type is constructed by creating a string by joining the words of the Size (Virtual machine size) with an underscore (_). In the screen shot below, these word are highlighted. The constructed string *for Standard F16s v2* is

Standard_F16s_v2.



Prerequisites

Installing and configuring FortiGate Autoscale for Azure requires knowledge of the following:

- Configuring a FortiGate using the CLI
- Azure deployment templates
- Azure Functions

It is expected that FortiGate Autoscale for Azure will be deployed by DevOps engineers or advanced system administrators who are familiar with the above.

Before you begin

Before starting the deployment, the following steps must be carried out:

1. Log into your Azure account. If you do not already have one, create one by following the on-screen instructions.
2. Create a service principal for Autoscale to interact with the different Azure services. The creation of the service principal may be done by a different Azure account.

The service principal requires *read* and *write* permissions which can be granted by adding the *Contributor* role to the service principal. In order to grant the service principal such permissions, the Azure account used to create the service principal requires the following permissions:

- *Microsoft.Authorization/roleAssignments/write* (to add role assignments)
- *Microsoft.Authorization/roleAssignments/delete* (to remove role assignments)

These permissions are included in the roles *User Access Administrator* and *Owner*. For details, refer to the Microsoft article Add or remove role assignments using Azure RBAC and the Azure portal.

Note the following items as you need them to deploy the Function App:

Item	Where to find it	Relevant FortiOS parameter
Application ID	You can find this item in Azure Active Directory > App registrations > (your app).	Service Principal App ID on page 70
Application secret	Only appears once. You cannot retrieve the application secret.	Service Principal App Secret on page 70
Object ID	Open the Azure CLI and enter the command `az ad sp show --id <the service principal client id>`. The object ID displayed may differ from the object ID displayed in Azure Active Directory > App registrations > (your-app). Use the value from the AzureCLI.	Service Principal Object ID on page 70

3. Confirm that you have a valid subscription to the PAYG and/or BYOL marketplace listings for FortiGate, as required for your deployment.

Without the valid subscriptions, the deployment will fail with errors.

Requirements when using an existing VNet

When using an existing VNet, ensure that the following FortiGate Autoscale for Azure requirements have been satisfied:

- IP address ranges in the VNets satisfy the Microsoft requirements listed in the article What address ranges can I use in my VNets?
- The VNet can contain 1 or more subnets but only up to 4 subnets can be used by the template deployment.
  - The FortiGate VMSS will be deployed in the subnet specified in Subnet 1 Name. This subnet will be referred as ‘Subnet 1’. This subnet must:
    - be a clean subnet (i.e. is not used by any other resource.)
    - have two service endpoints that have been manually enabled, one for Microsoft.AzureCosmosDB, and one for Microsoft.Web. If this requirement is not met, the template will automatically add the two service endpoints to the subnet (I.e. Subnet 1).
  - Up to 3 other subnets will be protected by the FortiGate VMSS.
- One Network Security Group is associated with Subnet 1.
- (Optional) One available (i.e. not associated with any resource) public IP address to be used for the external load balancer that will be created during template deployment.
  - This IP address must be of the 'standard' SKU in order to match the VMSS.
  - This requirement is optional as a new IP address can be created during template deployment, if the template parameter Frontend IP Address ID on page 68 is intentionally left empty.
- All the above components reside in the same resource group.
  - The location of the resource group should match the location of the deployment resource group.

Requirements when creating a new VNet

Subnet 1 is always required because the Autoscale VMSS is deployed into subnet 1. Subnets 2, 3, and 4 are optional. If created, they will be protected by the FortiGate VMSS. If you specify input for subnet 2, a subnet will be created and used as ‘subnet 2’. Similarly, ‘subnet 3’ and ‘subnet 4’ will be created if input is specified.

The following parameters are used to specify input:

- *Subnet 1 Address Range* is always required.
- *Subnet 1 Name* is used to enter a name of your choice. Leave it empty and a name will be generated.
- *Subnet 2/3/4 Address Range*, if provided, will assume the creation of subnet 2/3/4.
- *Subnet 2/3/4 Name* is used to enter a name of your choice. If the subnet is being created and this parameter is left empty, a name will be generated.

The parameters for subnet 2 to subnet 4 can be used in any combination. That is to say, the following combinations are valid:

- For a 2-subnet deployment:
  - Subnet 1 + subnet 2
  - Subnet 1 + subnet 3
  - Subnet 1 + subnet 4

- For a 3-subnet deployment:
  - Subnet 1 + subnet 2 + subnet 3
  - Subnet 1 + subnet 2 + subnet 4
  - Subnet 1 + subnet 3 + subnet 4
- For a 4-subnet deployment, subnet 1 + subnet 2 + subnet 3 + subnet 4 are used.

Obtaining the deployment package

The FortiGate Autoscale for Azure deployment package is located in the Fortinet Autoscale for Azure GitHub project. Navigate to the project release page and download `fortigate-autoscale-azure.zip` for the latest version.

Unzip this file on your local PC. Extracted content used in the deployment is described below:

Extracted Item	Description
assets	This folder contains *configset* files which can be modified as needed to meet your network requirements. For details on the allowable modifications, refer to the bullet for *The Blob Containers* in the section Appendix > Major components on page 106. In the section Uploading files to the Storage account on page 72 these files are loaded as the initial configuration of a new FortiGate-VM instance.
templates	This folder contains. deployment templates. The files `deploy_fortigate_autoscale.hybrid_licensing.*` are used to deploy FortiGate Autoscale for Azure.
fortigate-autoscale-azure-funcapp.zip	This is the function source file. This file should be uploaded to an online file host so that it is accessible to Azure. During the deployment you will specify the URL to this file in the parameter *Package Res URL on page 69*.

Deploying FortiGate Autoscale for Azure

Deploying FortiGate Autoscale for Azure involves Creating a template deployment on page 62 and Uploading files to the Storage account on page 72.

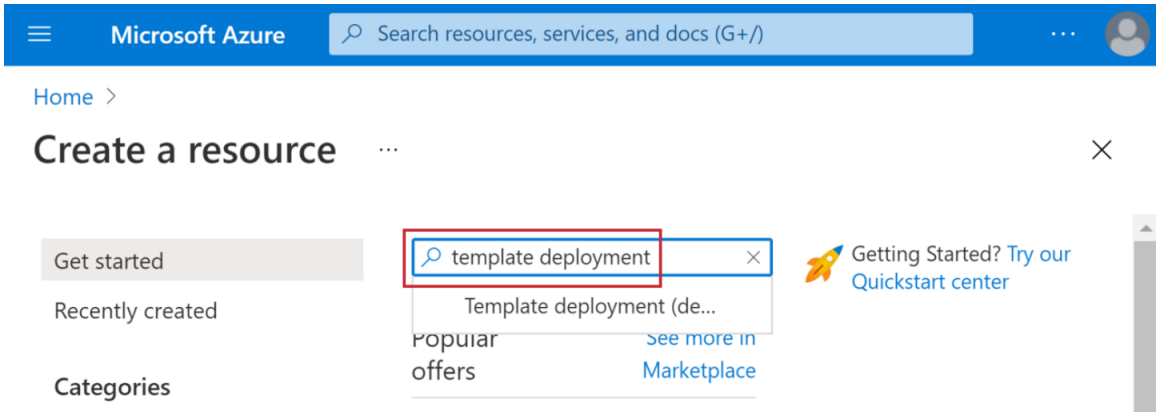
To deploy FortiGate Autoscale for Azure:

1. Create a template deployment using the template file `deploy_fortigate_autoscale.hybrid_licensing.json` and the parameter file `deploy_fortigate_autoscale.hybrid_licensing.params.json`.
2. Upload `configset` files to the Storage account.
3. If you will be using BYOL instances, upload `license` files to the Storage account.
4. Verify the deployment as described in the section Verifying the deployment on page 74.
5. Start the VMSS as described in the section Starting a VMSS on page 82.

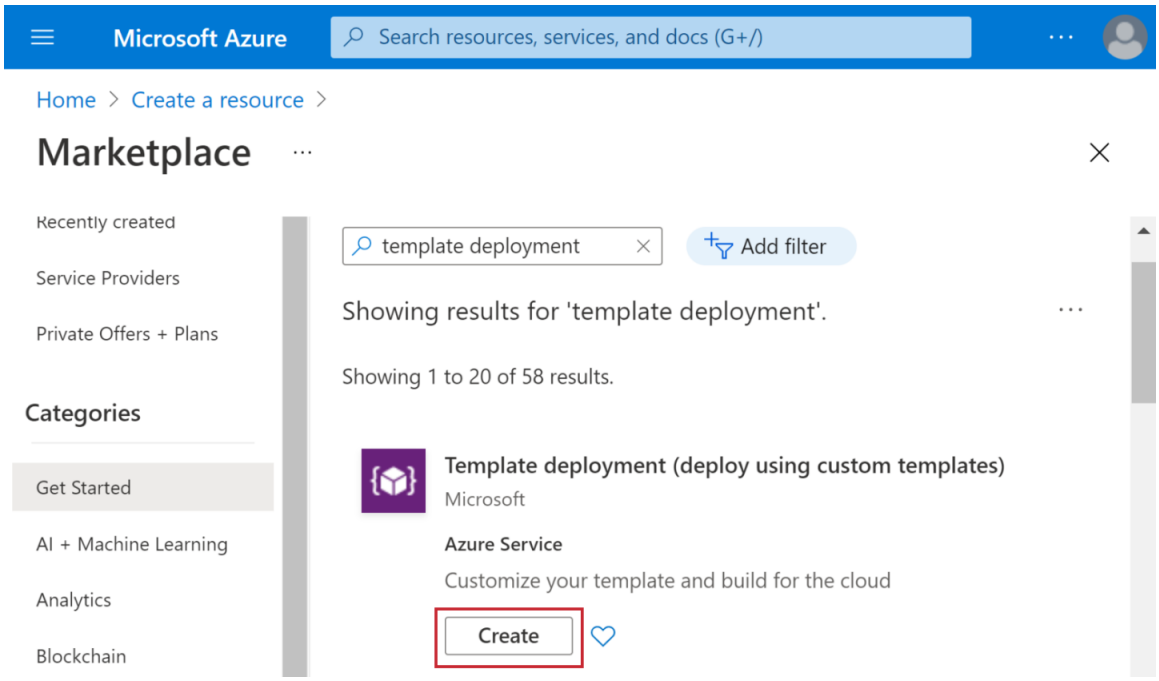
Creating a template deployment

To create a template deployment:

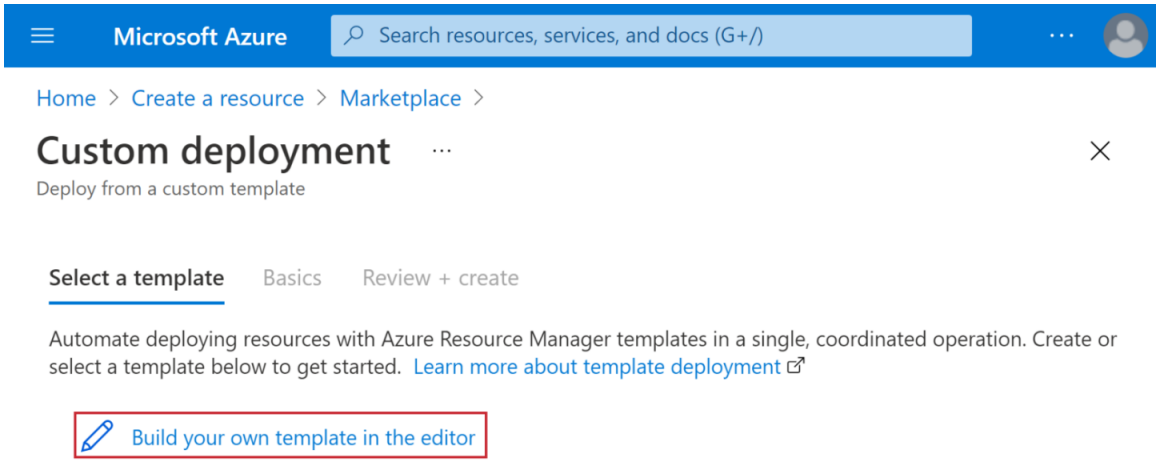
1. In the Azure portal, select *Create a resource* and search for "Template deployment".



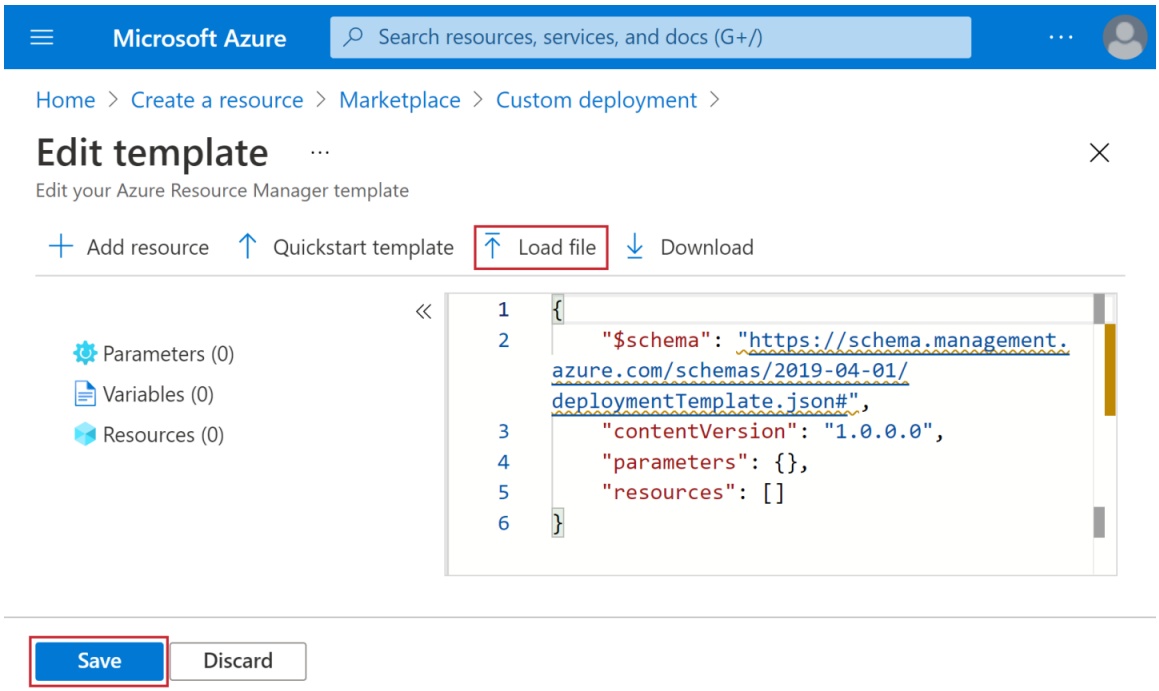
2. Click *Create*.



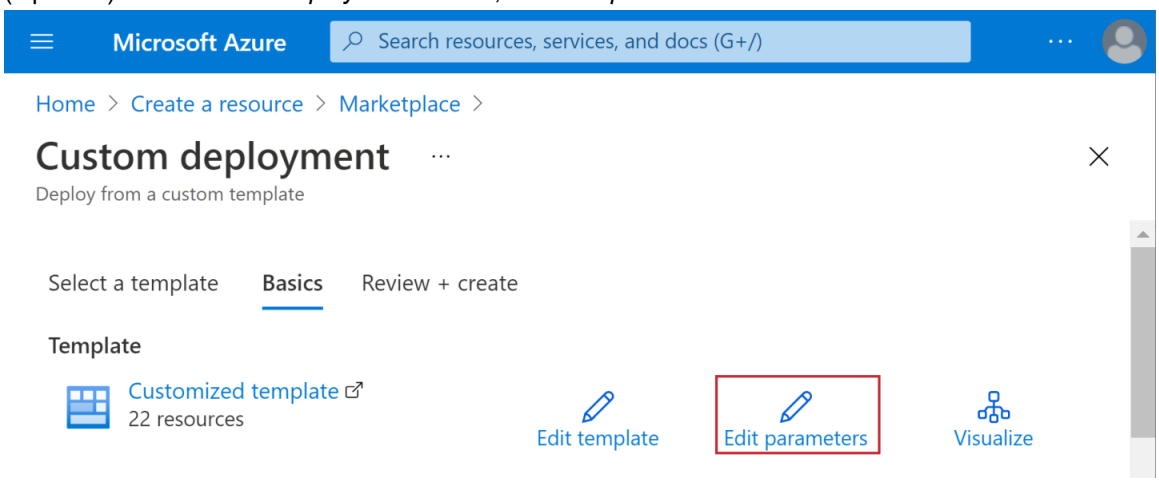
3. Click *Build your own template in the editor*.



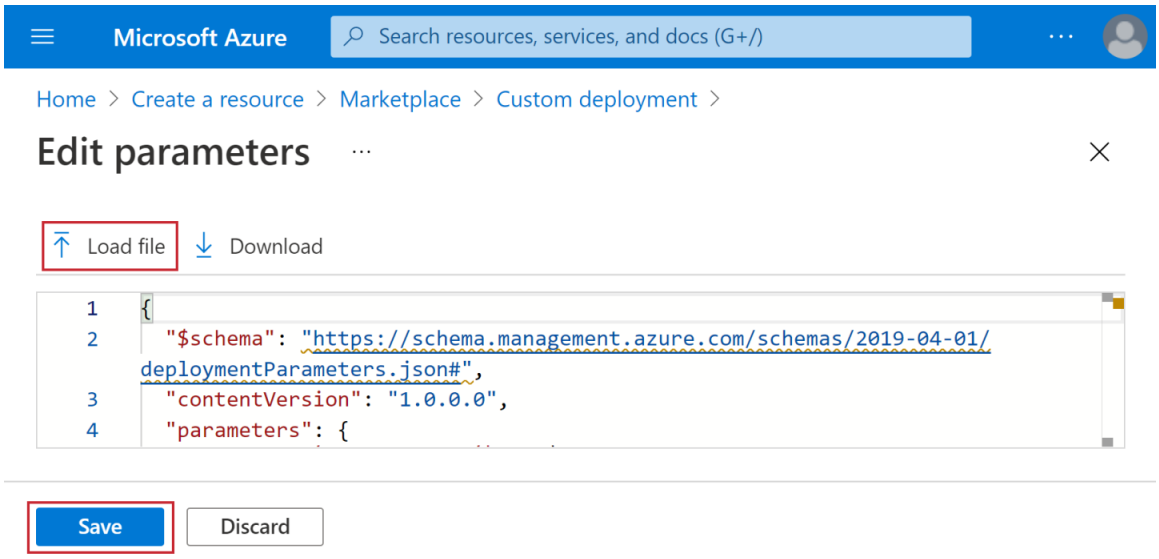
4. Click *Load file* to load the provided template file; then click *Save*.



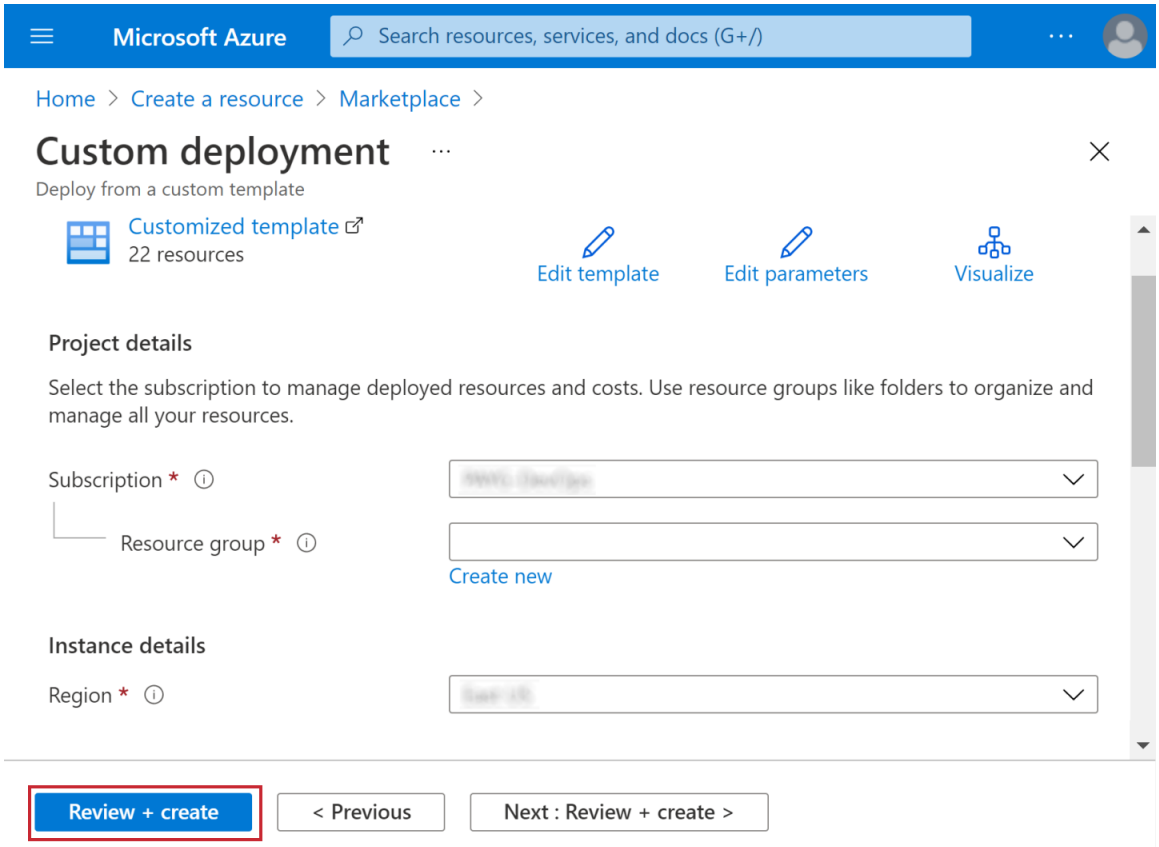
5. (Optional) In the *Custom deployment* screen, click *Edit parameters*.



Click *Load file* to load a predefined `.params.json` file; then click *Save*.

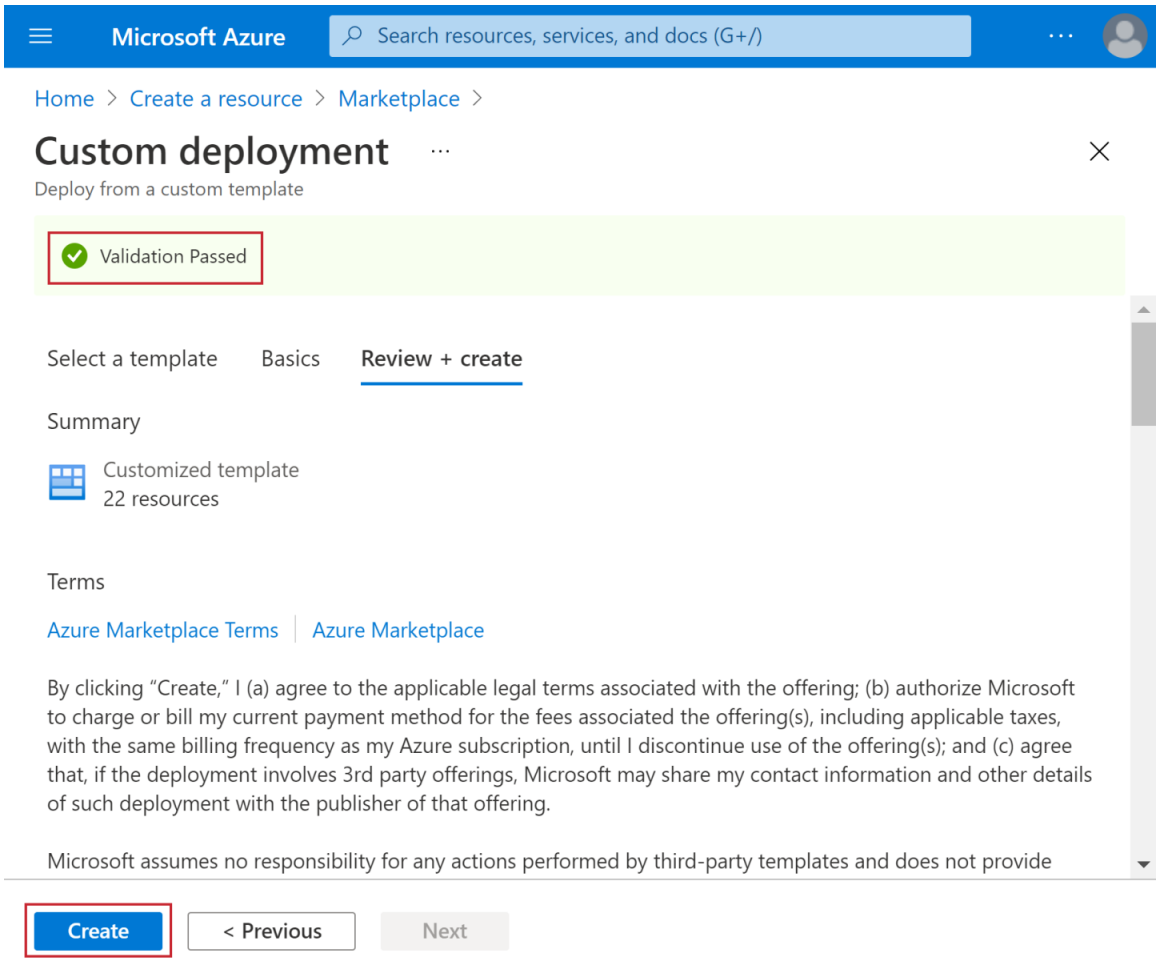


6. Review and update parameters. Parameter are described in the section Configurable variables on page 66.



7. Click *Review + create*. If parameter validation has not passed, click *Previous* and make the necessary corrections.

8. Review the Azure Marketplace Terms, optionally review the parameters again, and click *Create*.



Configurable variables

Following is a list of variables used during deployment and referenced throughout this guide.

Parameter name	Default value	Description
Subscription	Requires input	The Azure subscription FortiGate Autoscale for Azure will be deployed in.
Resource Group	Requires input	The resource group FortiGate Autoscale for Azure will be deployed in. Referred to as the *Autoscale resource group*.
Region	Requires input	The region in which the FortiGate Autoscale for Azure resources will be deployed in. Not every resource is available in every region.

Parameter name	Default value	Description
Access Restriction IP Range	Requires input	IP address ranges (single IPv4 address or Classless Inter-Domain Routing (CIDR) range) to allow access from the Internet or from your on-premises network to the CosmosDB and Function App. For security purposes, at least one entry must be specified. For multiple entries, each entry must be separated by a comma and no trailing comma is allowed.  0.0.0.0/0 accepts connections from any IP address. We recommend that you use a constrained CIDR range to reduce the potential of inbound attacks from unknown IP addresses.
Admin Password	Requires input	FortiGate administrator password on all VMs as well as the FortiAnalyzer if FortiAnalyzer integration is enabled. FortiGate and Azure VM password policy must be followed and the password must be11 - 26 characters in length with at least one uppercase letter, one lowercase letter, one digit, and one special character such as @ # $ % ^ & * - _ ! + =.
Admin Username	azureadmin	FortiGate administrator username on all VMs as well as the FortiAnalyzer if FortiAnalyzer integration is enabled.
BYOL Instance Count	2	Number of FortiGate instances the BYOL VMSS should have at any time. For High Availability in BYOL-only and Hybrid use cases, ensure at least 2 FortiGates are in the group. For specific use cases, set to 0 for PAYG-only, and >= 2 for BYOL-only or hybrid licensing.  Users can set the size to less than or equal to the number of valid licenses they own and the number should not exceed the *Max BYOL Instance Count*. Licenses can be purchased from FortiCare.
FortiAnalyzer Autoscale Admin Password	Requires input	Password for the FortiAnalyzer Autoscale Admin Username on page 67. The password must conform to the FortiAnalyzer password policy and have a minimum length of 8 and a maximum length of 128. If you need to enable KMS encryption, refer to the documentation.
FortiAnalyzer Autoscale Admin Username	Requires input	Name of the secondary administrator-level account in the FortiAnalyzer. FortiGate Autoscale uses this account to connect to the FortiAnalyzer to authorize any FortiGate device in the Auto Scaling group. To conform to the FortiAnalyzer naming policy, the user name can only contain numbers, lowercase letters, uppercase letters, and hyphens. It cannot start or end with a hyphen (-).
FortiAnalyzer Custom Private IP Address	Requires input	Custom private IP address to be used by the FortiAnalyzer. Must be within the Public subnet 1 CIDR range. Required if FortiAnalyzer Integration Options on page 68 is set to 'yes'. If FortiAnalyzer Integration Options on page 68 is set to 'no', any input will be ignored.
FortiAnalyzer Instance Type	Requires input	Size of the FortiAnalyzer-VM. For details on selecting the size, refer to the section Selecting the instance type on page 52

Parameter name	Default value	Description
		 Not all instance types are supported. Review FortiAnalyzer instance type support prior to selecting an instance.
FortiAnalyzer Integration Options	yes	Choose 'yes' to incorporate FortiAnalyzer into FortiGate Autoscale for Azure to use extended features that include storing logs into FortiAnalyzer.
FortiAnalyzer Public IP Address ID	Requires input	ID of the public IP address to associate with the FortiAnalyzer. If left empty, a new public IP address will be allocated in the resource group that contains the FortiAnalyzer.
FortiAnalyzer Version	6.4.5	FortiAnalyzer version supported by FortiGate Autoscale for Azure.
FortiGate PSK Secret	Requires input	Secret key used by FortiGate instances to securely communicate with each other. Must contain numbers and letters and may contain special characters. Maximum length is 128.  Changes to the PSK secret after FortiGate Autoscale for Azure has been deployed are not reflected here. For new instances to be spawned with the changed PSK secret, this environment variable will need to be manually updated.
FOS Version	7.0.1	FortiOS version supported by FortiGate Autoscale for Azure.
Frontend IP Address ID	Requires input	When the ID of a Public IP Address is provided, the Public IP Address will be used as the Frontend IP address associated with the external load balancer. If left empty, a new Public IP Address will be allocated in the resource group that contains the virtual network components.
Heart Beat Delay Allowance	30	Maximum amount of time (in seconds) allowed for network latency of the FortiGate heartbeat arriving at the Autoscale handler function. Minimum is 30.
Heart Beat Interval	60	Length of time (in seconds) that the FortiGate waits between sending heartbeat requests to the Autoscale handler function. Minimum is 30. Maximum is 120.
Heart Beat Loss Count	3	Number of consecutively lost heartbeats. When the Heart Beat Loss Count has been reached, the VM is deemed unhealthy and failover activities will commence.
Instance Type	Standard_F4	Size of the VMs in the VMSS. The default is Standard_F4. For more options, refer to the Microsoft article Sizes for virtual machines in Azure. For details on selecting the size, refer to the section Selecting the instance type on page 52

Parameter name	Default value	Description
Max BYOL Instance Count	2	Maximum number of FortiGate instances in the BYOL VMSS. For specific use cases, set to 0 for PAYG-only, and >= 2 for BYOL-only or hybrid licensing. This number must be greater than or equal to the Min BYOL Instance Count on page 69.  Users can set the size to match the number of valid licenses they own. Licenses can be purchased from FortiCare.
Max PAYG Instance Count	6	Maximum number of FortiGate instances in the PAYG VMSS. For specific use cases, set to 0 for BYOL-only, >= 2 for PAYG-only, and >= 0 for hybrid licensing. This number must be greater than or equal to the Min PAYG Instance Count on page 69.
Min BYOL Instance Count	2	Minimum number of FortiGate instances in the BYOL VMSS. For specific use cases, set to 0 for PAYG-only, and >= 2 for BYOL-only or hybrid licensing.  For BYOL-only and hybrid licensing deployments, this parameter must be at least 2. If set to 1 and the instance fails to work, the current FortiGate configuration will be lost.
Min PAYG Instance Count	0	Minimum number of FortiGate instances in the PAYG VMSS. For specific use cases, set to 0 for BYOL-only, >= 2 for PAYG-only, and >= 0 for hybrid licensing.  For PAYG-only deployments, this parameter must be at least 2. If it is set to 1 and the instance fails to work, the current FortiGate configuration will be lost.
PAYG Instance Count	0	Number of FortiGate instances the PAYG VMSS should have at any time. For High Availability in a PAYG-only use case, ensure at least 2 FortiGates are in the group. For specific use cases, set to 0 for BYOL-only, >= 2 for PAYG-only, and >= 0 for hybrid licensing.
Package Res URL	Requires input	Public URL of the function source file `fortigate-autoscale-azure-funcapp.zip`. The default value points to the source file available in the release assets of the GitHub repo `fortinet/fortigate-autoscale-azure`.  This URL must be accessible by Azure.
Primary Election Timeout	90	Maximum time (in seconds) to wait for the election of the primary instance to complete.

Parameter name	Default value	Description
Resource Name Prefix	Requires input	Prefix for all applicable resource names. Can only contain lowercase letters and numbers. Maximum length is 10.
Scale In Threshold	20	Percentage of CPU utilization at which scale-in should occur.
Scale Out Threshold	80	Percentage of CPU utilization at which scale-out should occur.
Service Plan Tier	Premium (P1V2)	Pricing tier for the function service plan.  The Free plan is for trial and demo only. Do not use it in a production environment.
Service Principal App ID	Requires input	*Application ID* for the Registered app used as the Autoscale Function App API request service principal. This is the value that was noted when creating a service principal in the section Prerequisites on page 59.
Service Principal App Secret	Requires input	Password (*Authentication key*) for the Registered app used as the Autoscale Function App API request service principal. This is the value that was noted when creating a service principal in the section Prerequisites on page 59.
Service Principal Object ID	Requires input	*Object ID* for the Registered app used as the Autoscale Function App API request service principal. This is the value that was noted when creating a service principal in the section Prerequisites on page 59.
Storage Account Type	Standard_LRS	Storage account type.
Subnet 1 Address Range	Requires input	Defines the *Subnet 1 Address Range* in CIDR notation. When creating a new VNet, the address range must be contained by the address space of the virtual network as defined in VNet Address Space on page 71. When using an existing VNet, the value must match the address range of the subnet specified in Subnet 1 Name on page 70. After deployment, the address range of a subnet which is in use can't be edited.
Subnet 1 Name		Name of subnet 1. The FortiGate Autoscale VMSS is deployed in this subnet. When creating a new VNet, the input value is used as the Subnet 1 name; if left empty, a name will be generated. When using an existing VNet, a valid non-empty input will assume the association of the target subnet with FortiGate Autoscale, and the target subnet will be associated as Subnet 1.
Subnet 1 Network Security Group Name	Requires input	Name of the Network Security Group (NSG) associated with the subnet 1. The FortiGate Autoscale VMSS is deployed in this subnet. Required when using an existing VNet. When creating a new VNet, any input will be ignored.
Subnet1 Network	1000	Starting number for the rule priority of the Network Security Group (NSG)

Parameter name	Default value	Description
Security Group Rule Priority		associated with subnet 1 where the Autoscale related rules will be deployed. When using an existing VNet, assign a number that does not conflict with the priority of any existing rule in the NSG specified in the Subnet 1 Network Security Group Name on page 70.
Subnet 2 Address Range	Conditionally requires input	The *Subnet # Address Range* parameters define the address range for the subnet, in CIDR notation. The address range must be contained by the address space of the virtual network as defined in VNet Address Space on page 71. • When creating a new VNet, a valid non-empty input will assume the creation of subnet #. • When using an existing VNet, the value should match the address range of the target subnet. After deployment, the address range of a subnet which is in use can't be edited.
Subnet 3 Address Range	Conditionally requires input	
Subnet 4 Address Range	Conditionally requires input	
Subnet 2 Name	Conditionally requires input	(Optional) The *Subnet # Name* parameters specify the name of the subnet. If subnet # is created, the FortiGate will have a network interface in this subnet. When creating a new VNet that contains the subnet, the input value is used as the Subnet # name. If left empty, a name will be generated. When using an existing VNet, a valid non-empty input will assume the association of the target subnet with FortiGate Autoscale, and the target subnet will be associated as 'Subnet #'.
Subnet 3 Name	Conditionally requires input	
Subnet 4 Name	Conditionally requires input	
VMSS Availability Zones		Availability zones to use "strict zone balancing", in array format. For example: [1], [1, 3], [1, 2, 3]. To use "best effort zone balancing", leave empty. If zone balancing is not applicable, set to a single zone - for example [2].  The template does not validate the input availability zone(s) against the region. To ensure the correct number of availability zones for your region, refer to the Microsoft articles Azure regions with availability zones and Zone Balancing.
VMSS Placement Groups	single	VMSS placement group options. For more information, please refer to the Microsoft article Create a virtual machine scale set that uses Availability Zones.
VNet Address Space		IP address space of the VNet in CIDR notation. E.g. 10.0.0.0/16. Required when using an existing VNet; the value should match the address space of the target VNet.
VNet Deployment Method	create new	Options for Virtual Network (VNet) deployment: • create new

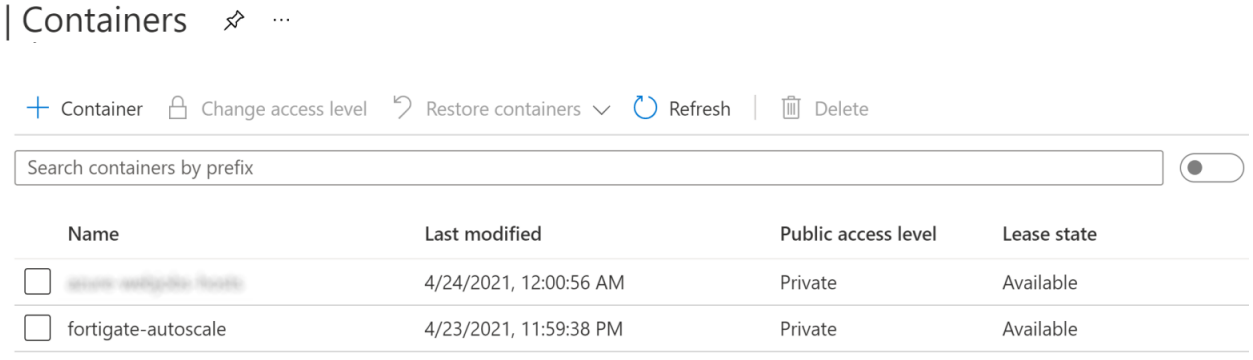
Parameter name	Default value	Description
		• use existing The VNet resource group (specified in the VNet Resource Group Name on page 72 parameter) must be in the same region as the Autoscale resource group (specified in the Configurable variables on page 66parameter). If using an existing VNet, refer to the section Requirements when using an existing VNet on page 60.
VNet Name	Conditionally requires input	Name of the Azure VNet to connect to FortiGate Autoscale. Required when using an existing VNet. When creating a new VNet, this parameter can be left empty and a name will be generated.
VNet Resource Group Name	Conditionally requires input	Name of the resource group that contains the VNet and related network components. Required if the VNet is not in the Autoscale resource group (specified in the parameter Resource Group on page 66). If not specified, the Autoscale resource group will be used. For details, refer to the description for the parameter VNet Deployment Method on page 71. This resource group must be in the same region as the Autoscale resource group.

Uploading files to the Storage account

The template deployment creates the storage container `fortigate-autoscale` in the resource group you selected or created in step 6 of the section Creating a template deployment on page 62.

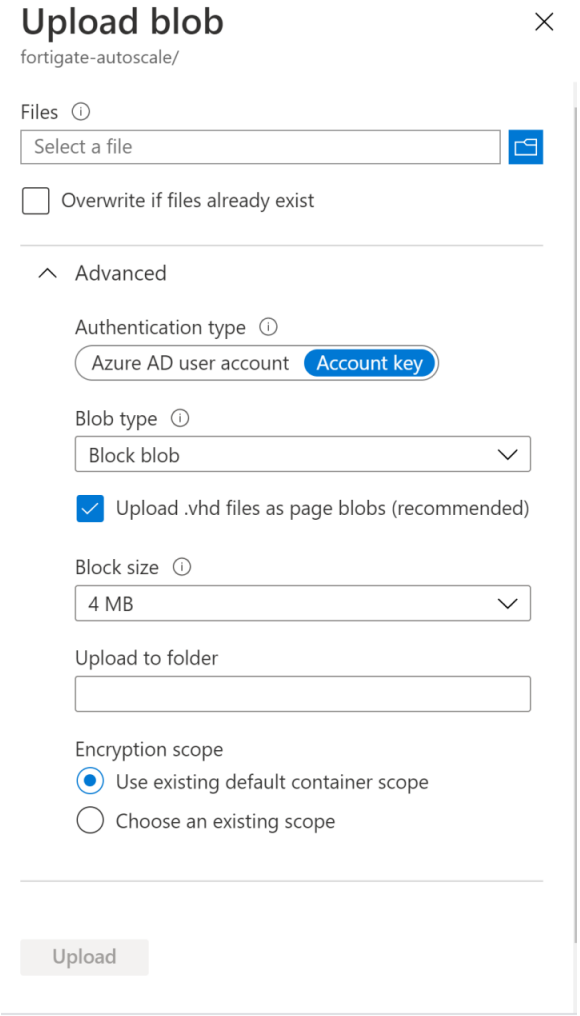
To upload files to the storage container:

1. From the Resource group, load the Storage account by clicking its name.
2. From the Storage account navigation column, under *Data storage*, click *Containers*. The `fortigate-autoscale` container will be listed.



3. Click the `fortigate-autoscale` container.

4. Click *Upload*.
5. In the *Upload blob*, click *Advanced* to display more options.



6. Specify the folder to upload to in *Upload to folder*:
   - For *configset* files, enter `assets/configset`.
   - For *license* files, enter `assets/license-files/fortigate`.
7. Select a file or files to upload:
   - For *configset* files, select all the files in the *configset* folder of the deployment package.
   - For *license* files, select your BYOL license file(s).

   If you provide two license files with the same content, only one of them will be used, the other one will be ignored.

   If you upload a file with the same name but different content, there are two outcomes:
   - If the old license has not been distributed, the new file replaces the old one.
   - If the old license has been distributed, the new file is treated as a new license. The old license is still valid, but it cannot be redistributed in the future.
8. Click *Upload*.

Verifying the deployment

FortiGate Autoscale for Azure deploys the following components:

- 1 Public Load balancer
  - This load balancer will be associated with the FortiGate subnet and the Frontend Public IP address to receive inbound traffic.
- 1 Internal Load balancer
- 1 Network security group
- 1 Virtual machine scale set for BYOL
- 1 Virtual machine scale set for PAYG
- 1 Virtual network (only if deployed with creating a new virtual network)
- 1 Public IP address
- 1 Azure Cosmos DB account
- 1 Function App
- 1 Application Insights (automatically enabled if your region supports it)
- 1 App Service plan
- 1 Key vault
- 1 Storage account

If deploying with FortiAnalyzer integration, the following are also deployed:

- 1 Virtual machine for FortiAnalyzer
- 1 virtual machine for the FortiAnalyzer
- 1 network interface for the FortiAnalyzer
- 1 Public IP address for the FortiAnalyzer (only if FortiAnalyzer Public IP Address ID on page 68 is left empty)
- 2 Disk components for use by FortiAnalyzer

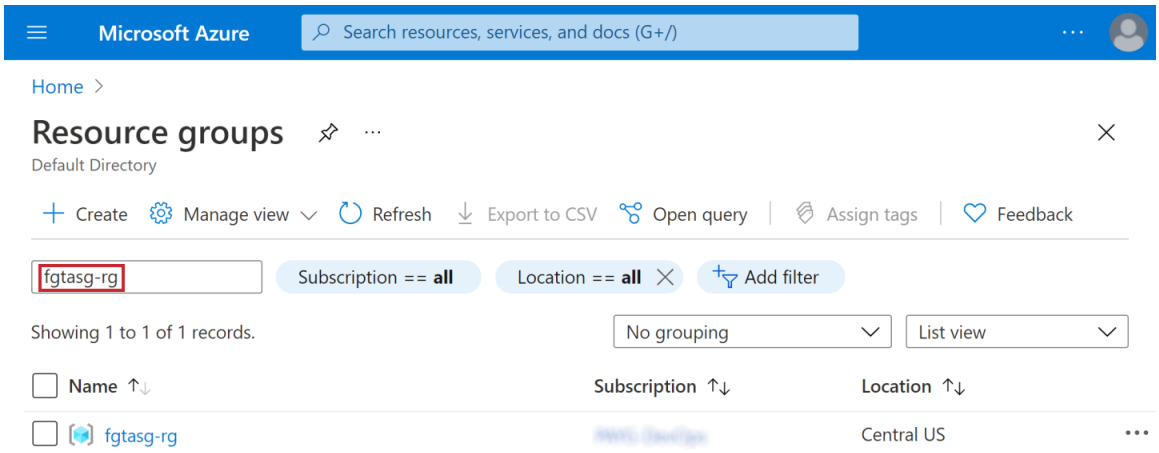
For deployments that have two resource groups, the network related components are deployed to the VNet resource group and the DB, Storage account, and Function App related components are deployed to the Autoscale resource group.

FortiGate Autoscale for Azure is fully deployed once you verify the following components:

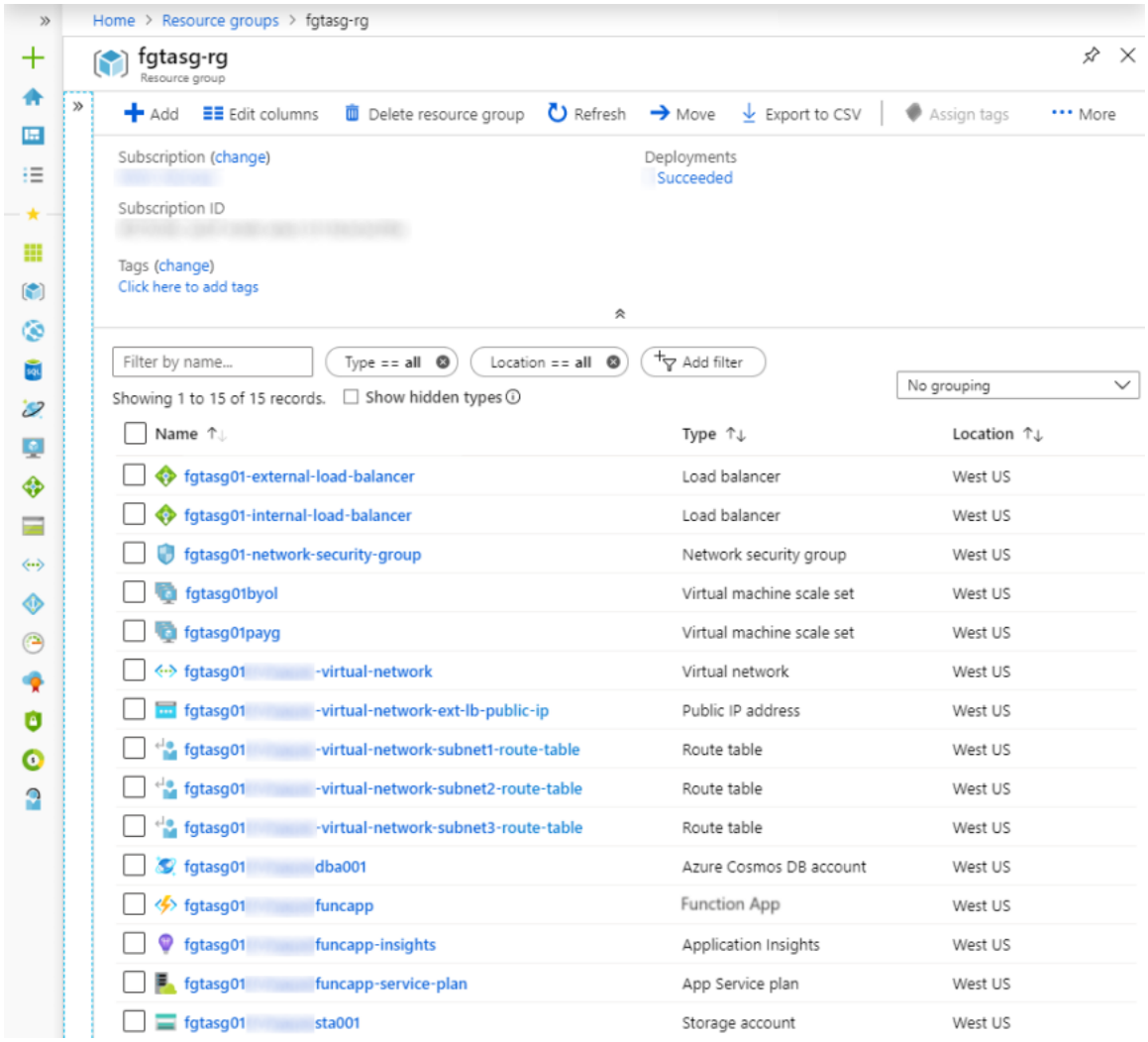
- the Function App
- the database
- the primary election

To load a resource group:

1. In the Azure console, from the left navigation column, select *Resource groups*.
2. Locate the resource group you wish to load by scrolling through the list or by using one or more of the name, subscription, and location filters. In the example below, this is *fgtasg-rg*.

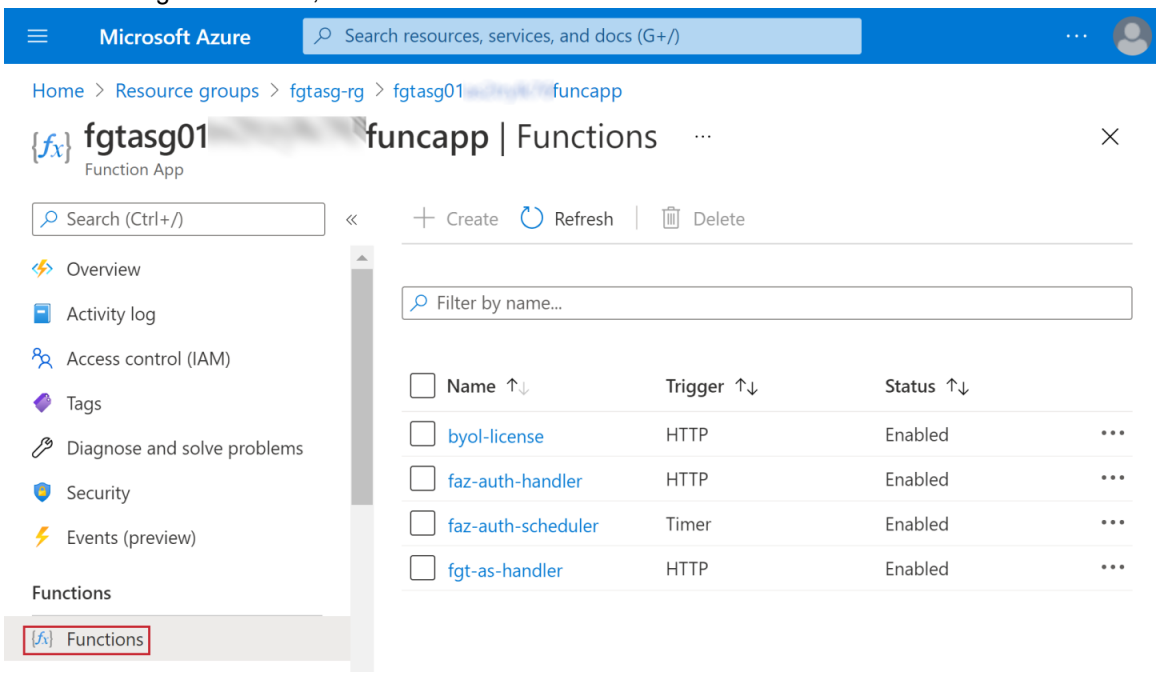


3. Click the name to load the resource group *Overview* page. In the example deployment, the VNet resource group is the same as the Autoscale resource group.



To verify the Function App:

1. From the Autoscale resource group *Overview* page, load the Function App by clicking the name of the item of type *Function App*.
2. From the navigation column, select *Functions*.



You should see four functions on the right:

- *byol-license*: The function to distribute BYOL licenses.
- *faz-auth-handler*: The function to handle authorization of FortiGate in the FortiAnalyzer.
- *faz-auth-scheduler*: The function to handle authorization of FortiGate in the FortiAnalyzer on a timely basis.
- *fgt-as-handler*: The main autoscaling function.

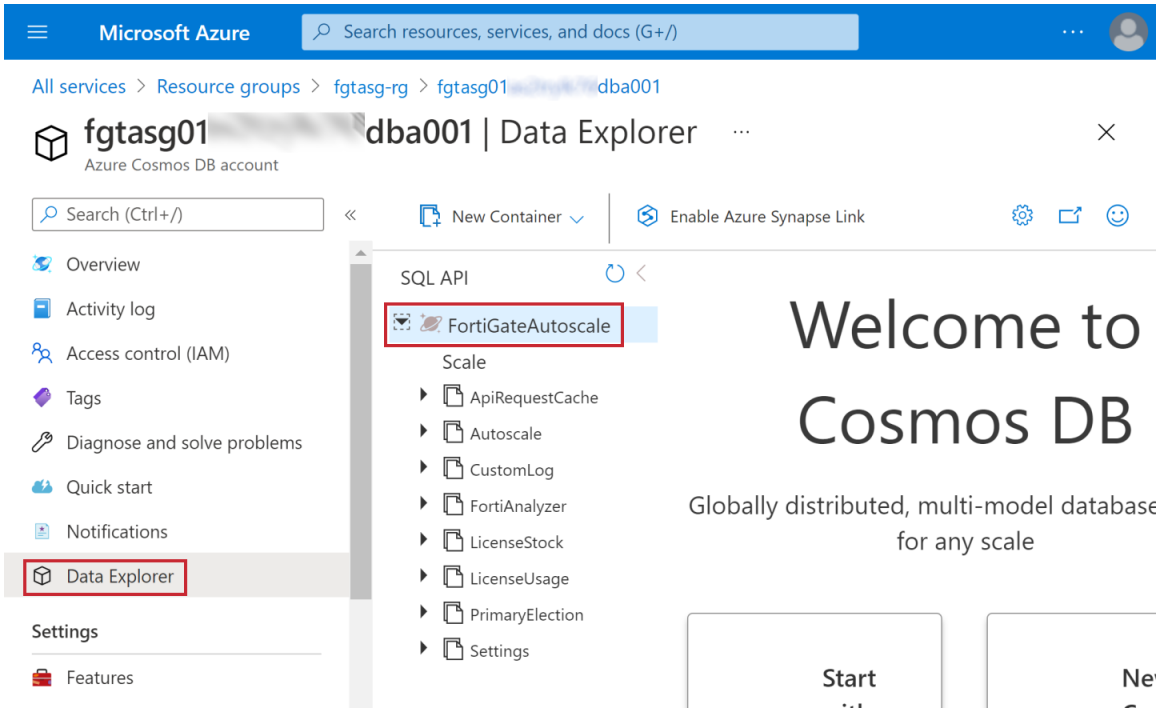
To verify the database:

1. From the Autoscale resource group *Overview* page, click the *Azure Cosmos DB account* name.
2. From the navigation column, click *Data Explorer*.
3. Expand the database *FortiGateAutoscale*.

You will see the following database and tables:

- *Database:* FortiGateAutoscale
- *Tables:*
  - ApiRequestCache
  - Autoscale
  - CustomLog
  - FortiAnalyzer
  - LicenseStock
  - LicenseUsage
  - PrimaryElection
  - Settings

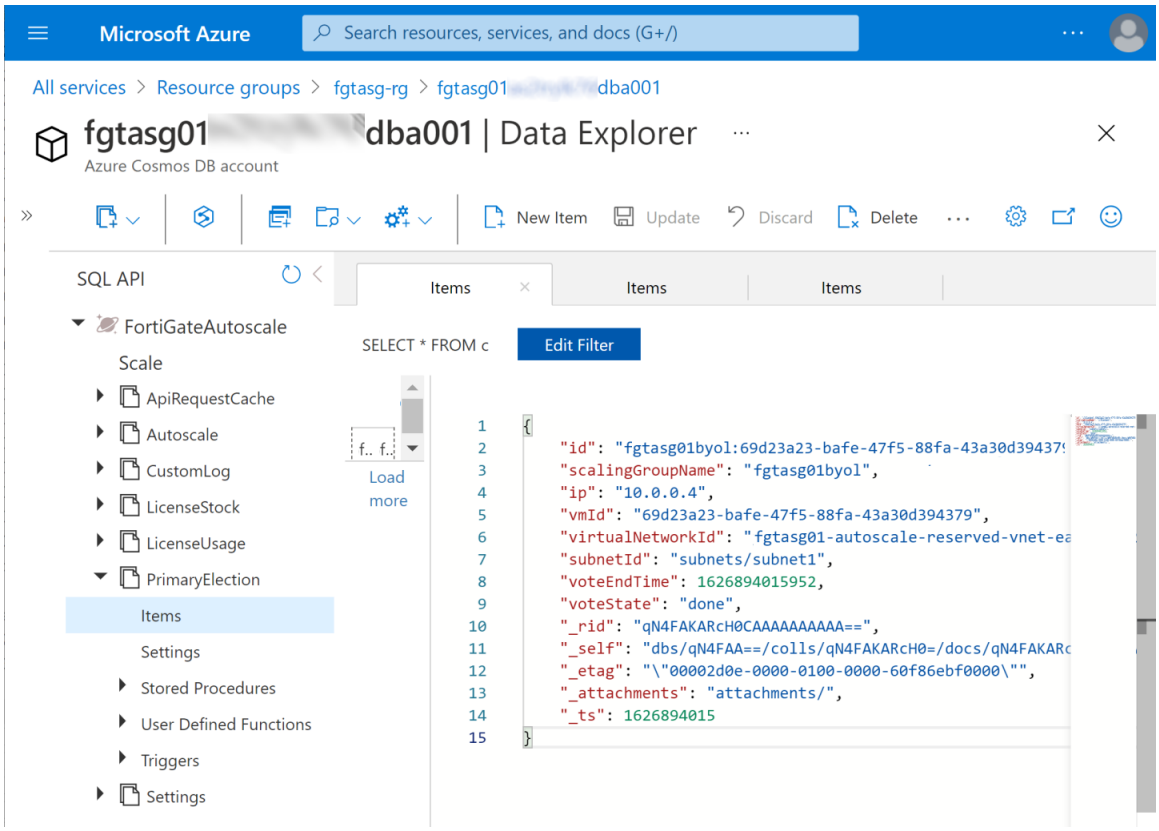
The database *Data Explorer* page will look as shown below:



To verify the primary election:

The elected primary FortiGate-VM will be logged in the CosmosDB *FortiGateAutoscale* in the table *FortiGatePrimaryElection*.

1. Expand the *FortiGatePrimaryElection* table and click on *Items*.
2. There will be one item in the table, select it.



- *id* is the unique identifier of a database record.
- *scalingGroupName* is the name of the Scale Set in which the primary FortiGate-VM is located.
- *ip* is the primary private IP address of the current primary FortiGate-VM.
- *vmId* is the index of the FortiGate-VM in the Scale Set.
- *virtualNetworkID* is the ID of the Virtual Network in which the primary FortiGate-VM instance is located.
- *subnetId* is the ID of the subnet in which the primary FortiGate-VM is located.
- *voteEndTime* is the Unix time stamp for when this primary election should expire if the vote state cannot change to *done* by this time.
- *voteState* is the state of the voting process.
  - *pending*: election of the primary instance is still in progress. You should wait for its completion. At this point in time, the final primary instance is not yet known.
  - *done*: the primary election process has completed.

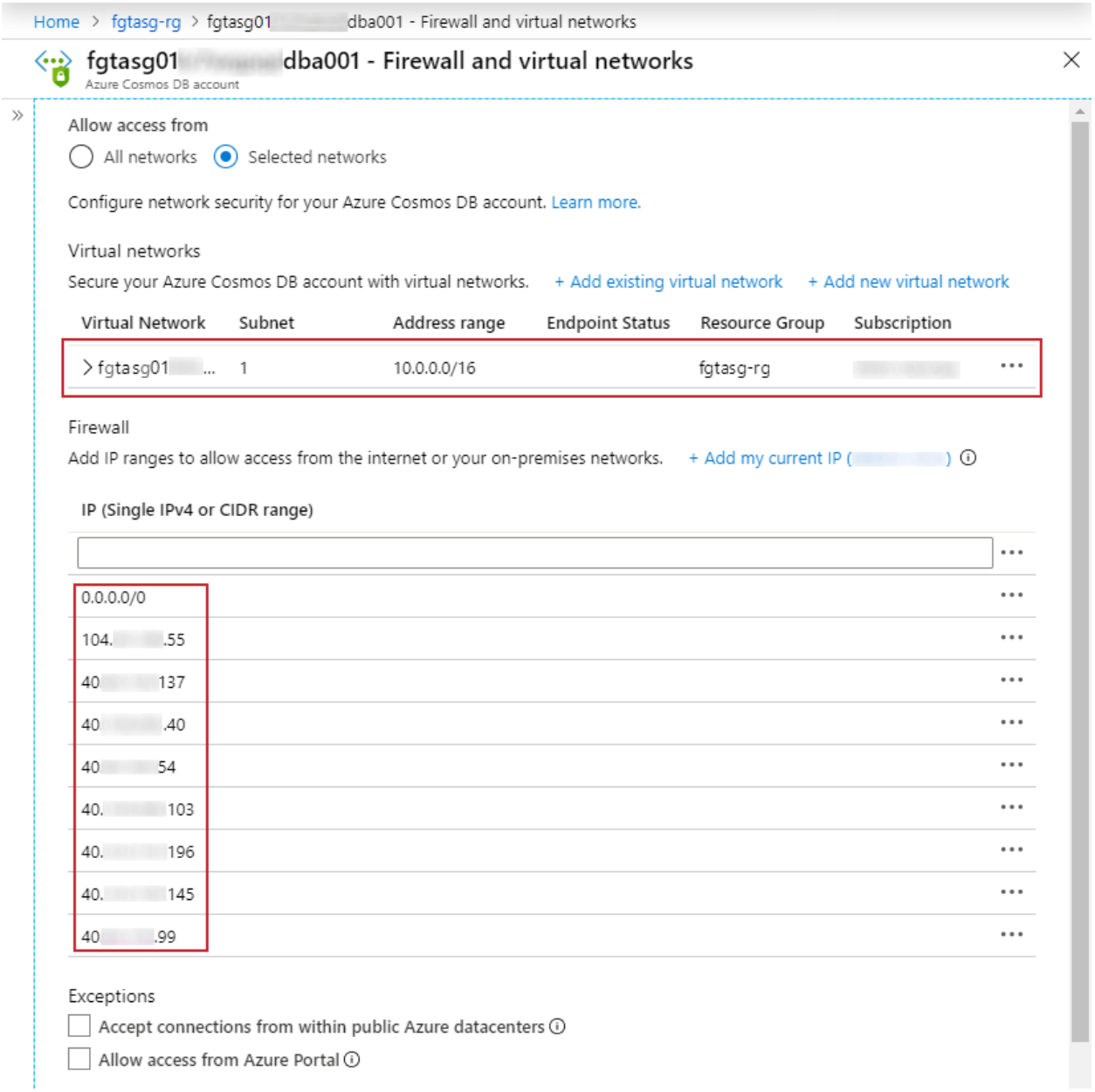
Security features for network communication

Security features are automatically enabled and configured as described in the following sections.

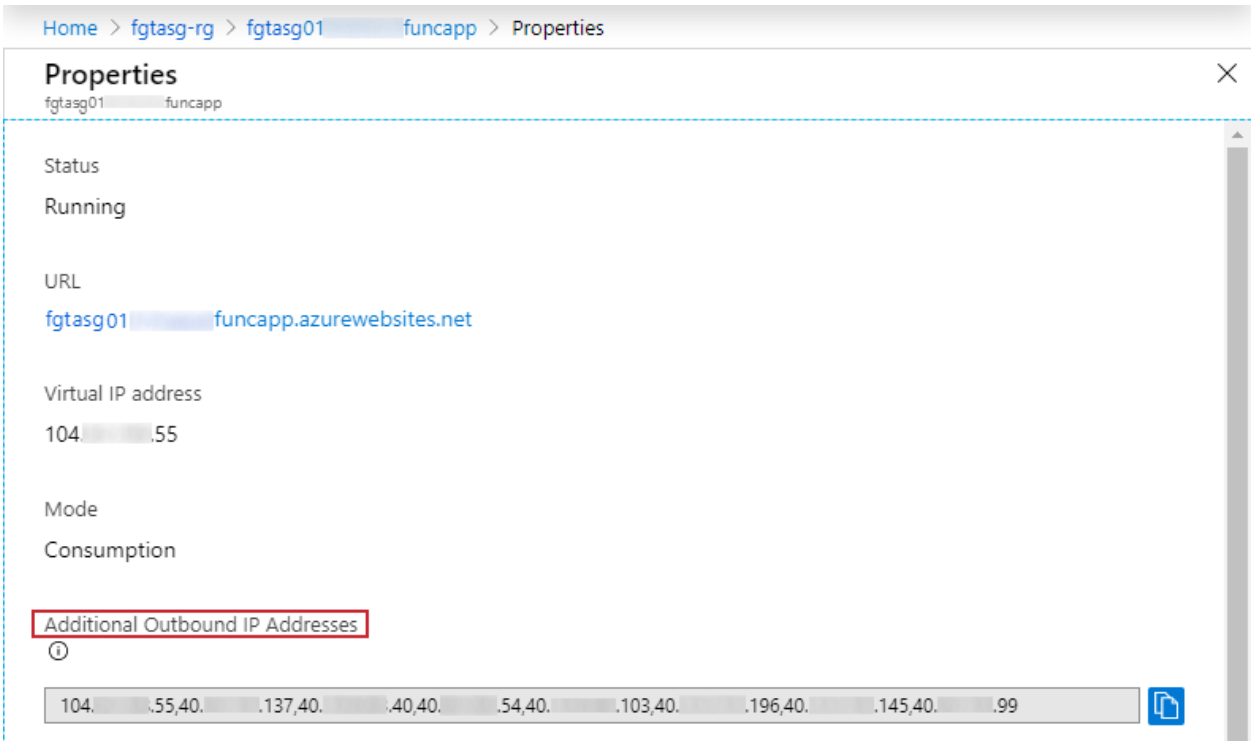
Database

Firewalls are set for IP address ranges and the VNet. The firewall only allow interactions with the DB tables from the FortiGate subnet, Function App additional outbound IP addresses, and user-defined IPv4 IP ranges.

To view the firewalls, load the Cosmos DB. From the *Settings* section of the left navigation tree, click *Networking* and then click *Firewall and virtual networks*.



The IP addresses listed in the Firewall section include the set of all possible Function App outbound IP addresses as obtained from the *Additional Outbound IP Addresses* field of the Function App *Properties*. To view these IP addresses, load the Function App, click the *Platform features* tab and then click *Properties*. Each IP address in the list has been added as an entry in the Cosmos DB firewall.

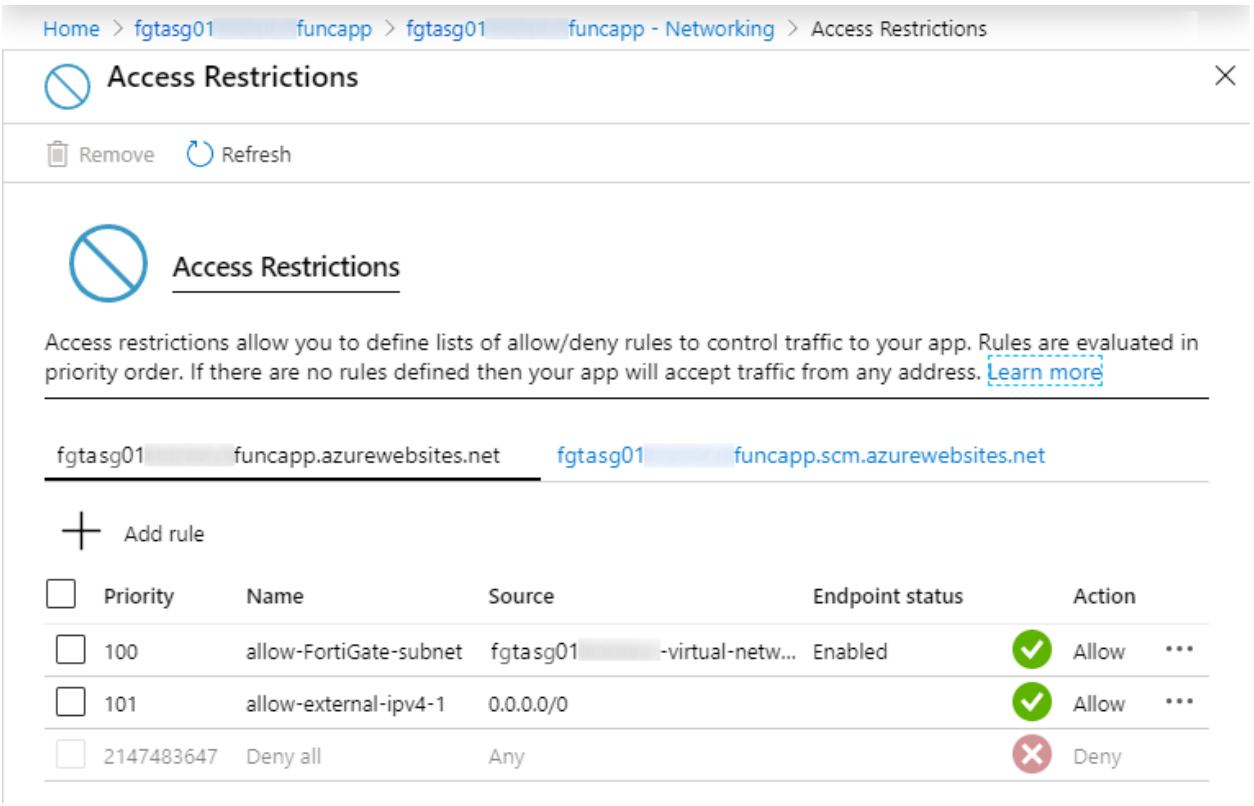


If Function App *Additional Outbound IP Addresses* change, the Cosmos DB firewall must be manually updated so that each IP address has a corresponding entry in the Cosmos DB firewall. Any IP address not listed in the Cosmos DB firewall will be blocked, thus causing the Autoscale function to be blocked. For details on when Function App outbound IP addresses change, refer to the Microsoft article When outbound IPs change.

Function App

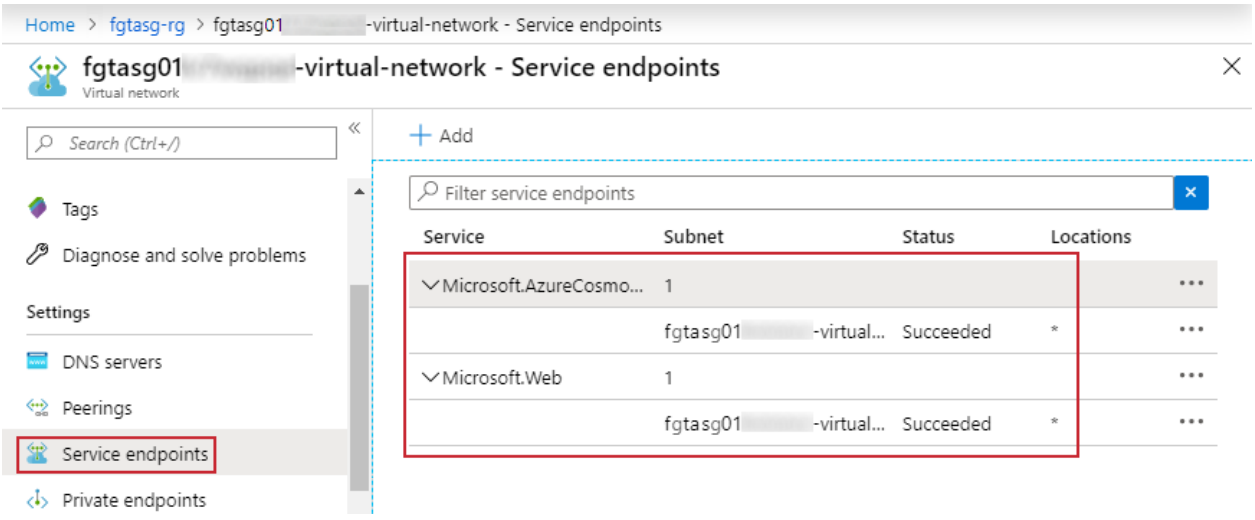
Requests are restricted by source. Incoming requests are only allowed from the FortiGate subnet and from user-defined IPv4 IP ranges.

To view *Access Restrictions*, load the Function App. In the right hand pane, click the *Platform features* tab and then click *All settings*. From the *Settings* section of the left navigation tree, click *Networking* and then click *Configure Access Restrictions*.



Virtual Network

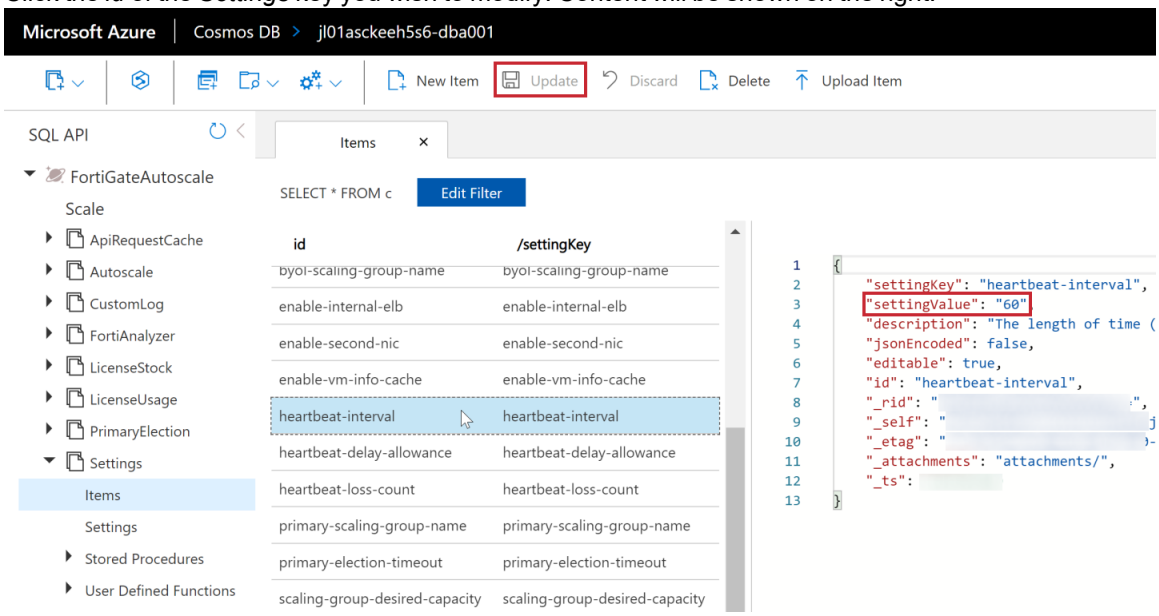
The service endpoints for Azure services are enabled. Service endpoints should be enabled for the minimum number of Azure services required for Autoscale.



Modifying the Autoscale settings in Cosmos DB

To modify Autoscale settings:

1. Locate the Autoscale settings in the *FortiGate Autoscale* database. For details, refer to the section To verify the database: on page 76.
2. Expand the Settings container
3. Click the *id* of the *Settings* key you wish to modify. Content will be shown on the right:



4. Update the value of the property *settingValue*.
5. Click on the *Update* button located on the menu bar above.

Each Autoscale setting has a property of *editable*. It is recommended that items with *editable* set to *false* not be modified.

If it is necessary to modify one of these settings (for example, the FortiAnalyzer IP address has changed), please leave a question in the GitHub project *Issues* tab so that assistance can be provided.

Starting a VMSS

Your deployment will have two Virtual machine scale sets (VMSS), one for BYOL instances and one for PAYG instances. For deployments using only one instance type, start that VMSS. For Hybrid licensing deployments, start both VMSS.

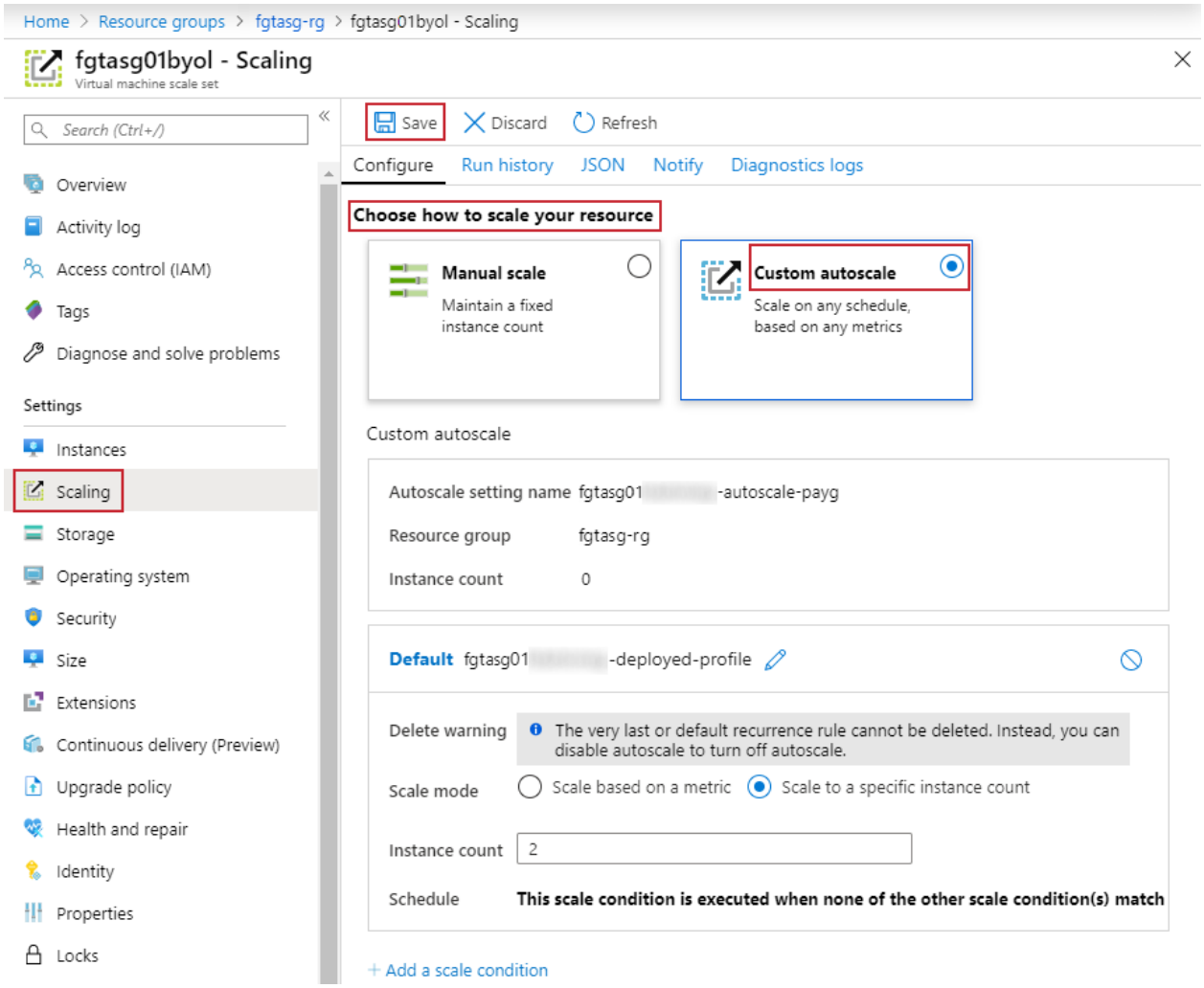
To start a VMSS:

1. Load the resource group that contains the VMSS. In deployments with one resource group, this value is specified in the *Resource group* parameter in step 6 of the section Creating a template deployment on page 62. If your

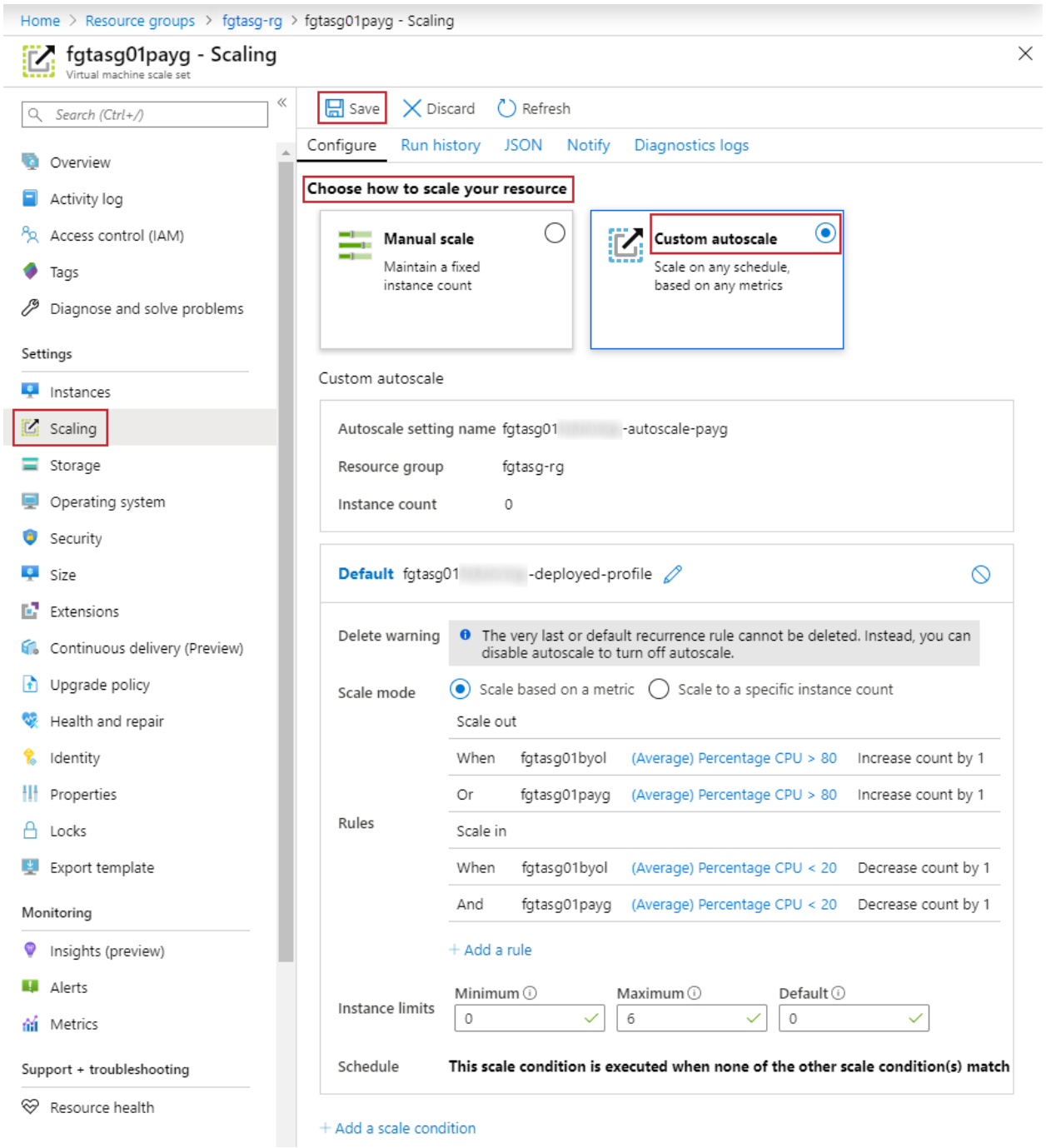
deployment has a separate resource group for the VNet, load that one instead. That resource group is specified in the VNet Resource Group Name on page 72 parameter.

2. Load the *Virtual machine scale set* by clicking its name.
3. From the Virtual machine scale set account navigation column, under *Settings*, click *Scaling*.
4. Under *Choose how to scale your resource*, click *Custom autoscale*.
5. Adjust values as required.
6. Click *Save*.

The BYOL *Custom autoscale* appears as shown in the image:



The PAYG *Custom autoscale* appears as shown in the image:


Home > Resource groups > fgtasg-rg > fgtasg01payg - Scaling
fgtasg01payg - Scaling
Virtual machine scale set
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Instances
Scaling
Storage
Operating system
Security
Size
Extensions
Continuous delivery (Preview)
Upgrade policy
Health and repair
Identity
Properties
Locks
Export template
Monitoring
Insights (preview)
Alerts
Metrics
Support + troubleshooting
Resource health
Save
Discard
Refresh
Configure
Run history
JSON
Notify
Diagnostics logs
Choose how to scale your resource
Manual scale
Maintain a fixed instance count
Custom autoscale
Scale on any schedule, based on any metrics
Custom autoscale
Autoscale setting name fgtasg01 -autoscale-payg
Resource group fgtasg-rg
Instance count 0
Default fgtasg01 -deployed-profile
Delete warning
The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.
Scale mode
Scale based on a metric
Scale to a specific instance count
Rules
Scale out
When fgtasg01byol (Average) Percentage CPU > 80 Increase count by 1
Or fgtasg01payg (Average) Percentage CPU > 80 Increase count by 1
Scale in
When fgtasg01byol (Average) Percentage CPU < 20 Decrease count by 1
And fgtasg01payg (Average) Percentage CPU < 20 Decrease count by 1
Add a rule
Instance limits
Minimum
Maximum
Default
0
6
0
Schedule
This scale condition is executed when none of the other scale condition(s) match
Add a scale condition

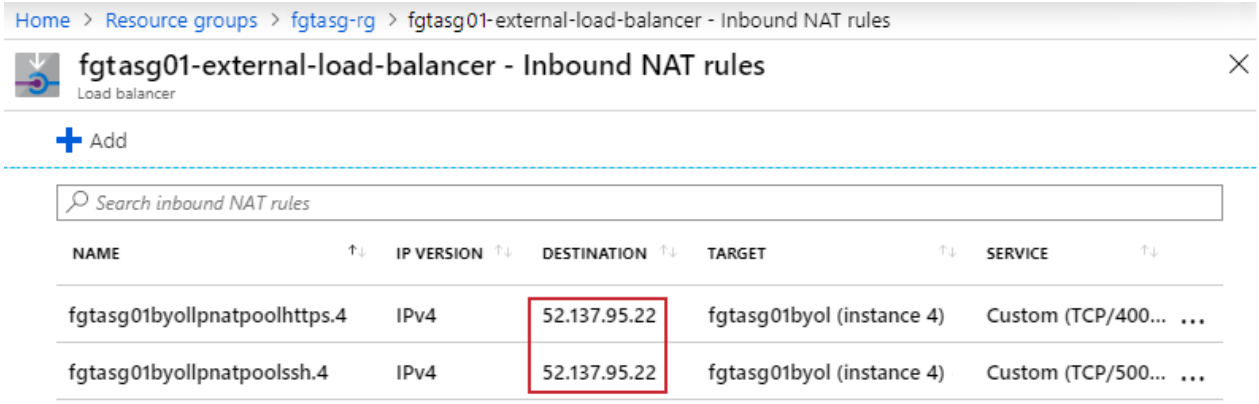
Connecting to the FortiGate-VM instances

To connect to a FortiGate-VM, you can use SSH commands or the web GUI using HTTPS with the IPv4 public IP address.

From the resource group *Overview* page, click the external load balancer name to load it. From the navigation column, click *Inbound NAT Rules*. For each instance in the scale set you will see two rules:

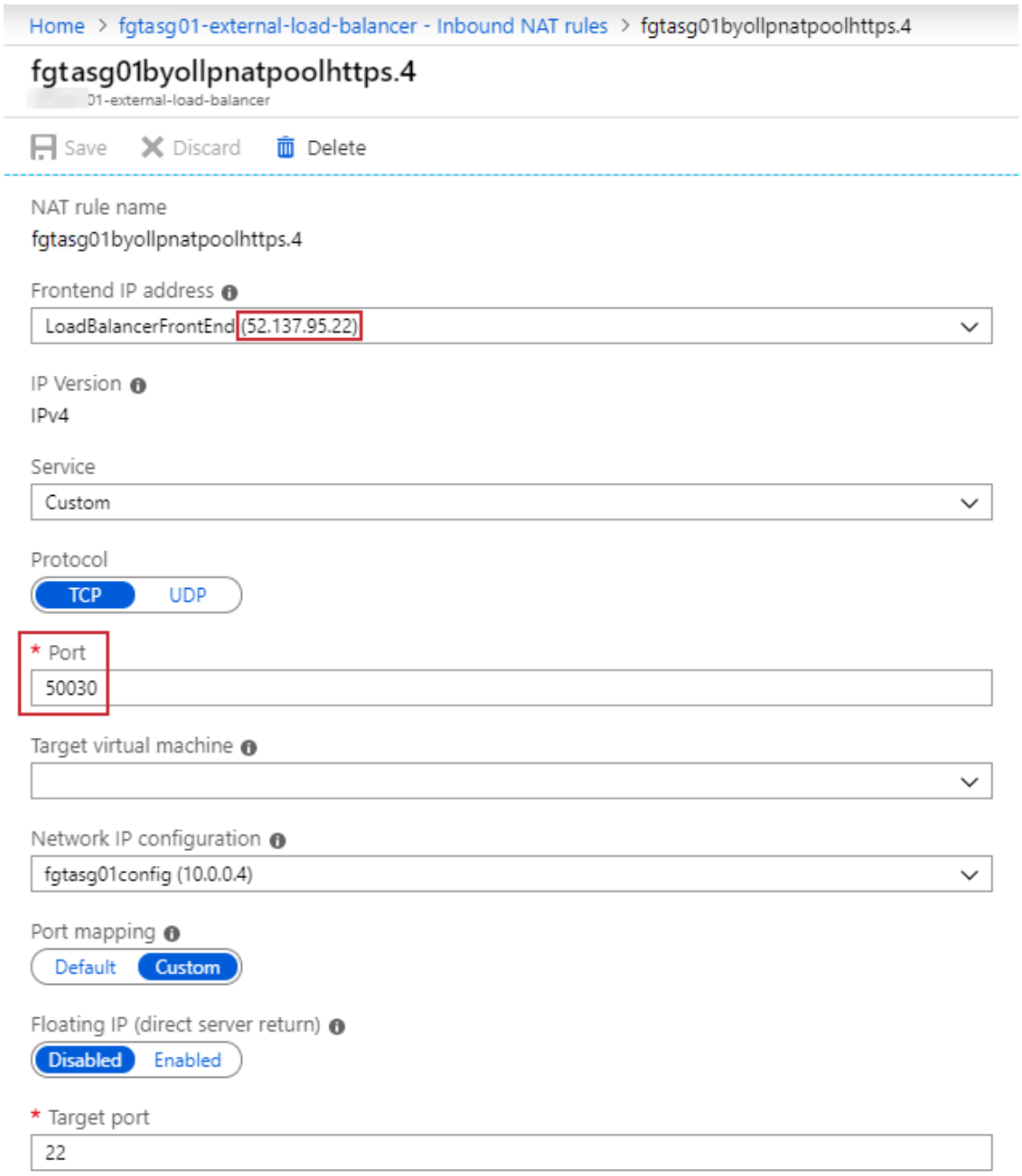
- One rule for SSH access to the instance.
- One rule for HTTPS access to the instance.

The *Inbound NAT Rules* page will look as shown below:



To access a FortiGate-VM instance, you need the Frontend IP address and port number of the instance you wish to connect to. The Frontend IP address is listed on the *Inbound NAT Rules* page. To obtain the port number, click the entry for the method you will use to access the instance (SSH or HTTPS). The port number will be listed midway down the page. (The IP address is also listed).

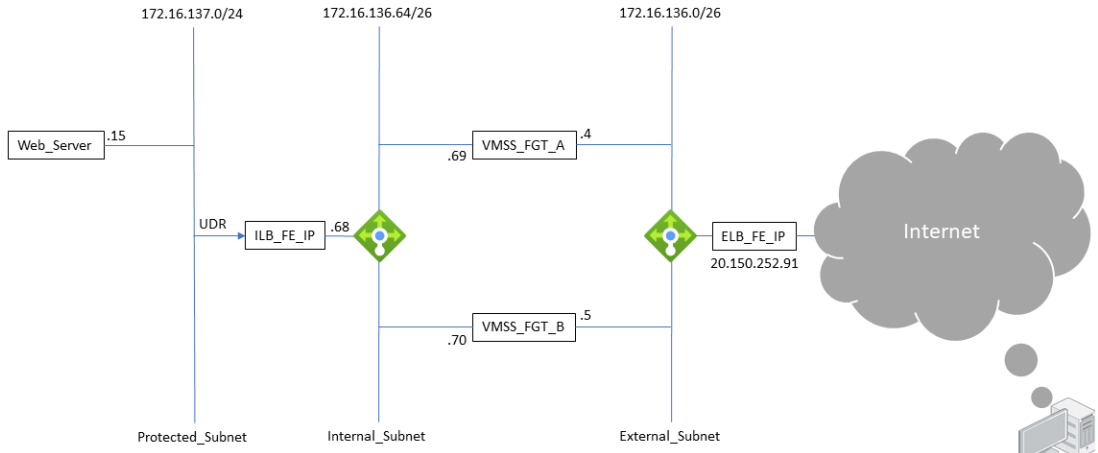
An example of an SSH access rule is shown below:



Configuring FGSP session sync

FortiGate session life support protocol (FGSP) `standalone-cluster` and `session-pickup` is automatically enabled on FortiGate-VM instances deployed on Azure with autoscaling enabled.

You can achieve the setup in this example by deploying the template available on GitHub.



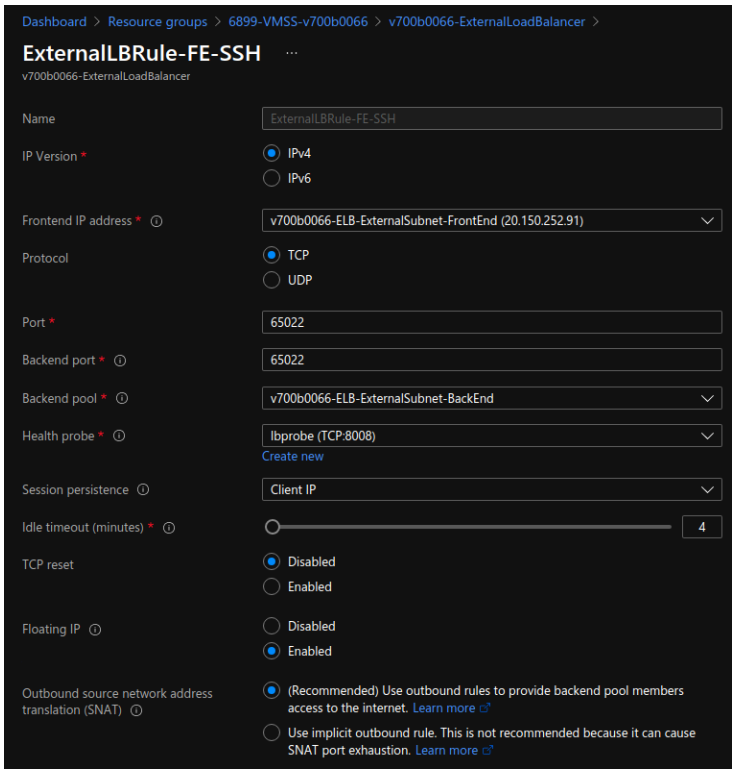

```
packet@1804:~$ az network route-table route show -g $RG --route-table-name v700b0066-ProtectedSubnet-RouteTable --name toDefault
{
  "addressPrefix": "0.0.0.0/0",
  "etag": "W/\"dc7d3637-fbcd-4461-b6dc-e6f8062eab2b\"",
  "hasBgpOverride": false,
  "id": "/subscriptions/4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a/resourceGroups/6899-VMSS-v700b0066/providers/Microsoft.Network/routeTables/v700b0066-ProtectedSubnet-RouteTable/routes/toDefault",
  "name": "toDefault",
  "nextHopIpAddress": "172.16.136.68",
  "nextHopType": "VirtualAppliance",
  "provisioningState": "Succeeded",
  "resourceGroup": "6899-VMSS-v700b0066",
  "type": "Microsoft.Network/routeTables/routes"
}
packet@1804:~$
```

The following describes the example configuration:

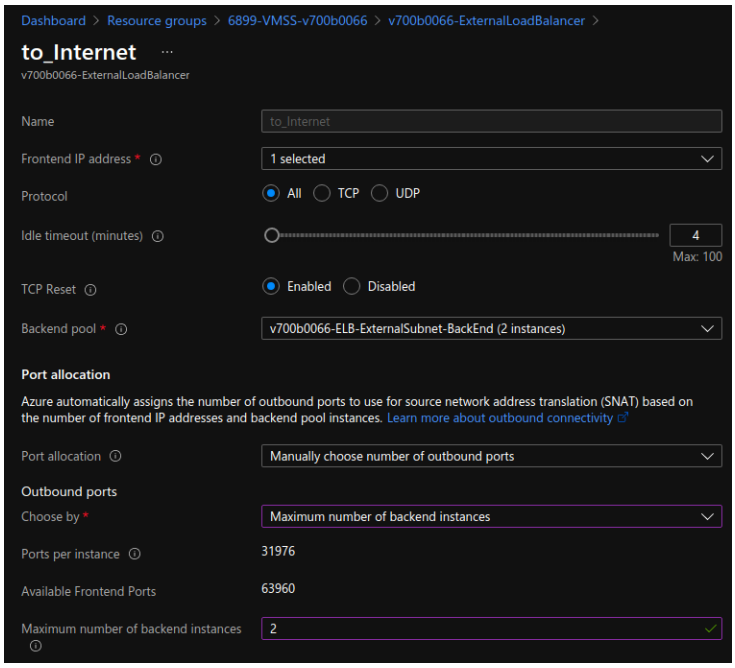
- The load balancing (LB) rules of both the external load balancer (ELB) and internal load balancer (ILB) have a floating IP address enabled and session persistence set to the client IP address.
- Outbound rules are configured to the ELB so that PC15 has internet access.
- The FortiGate-VMs have firewall virtual IP address rules configured with the ELB performing destination network address translation so that client access from the Internet to PC15 keeps the original IP address.
- Client access from the Internet to PC15 has symmetric flow.

To configure FGSP session sync on FortiGate-VMs on Azure with autoscaling enabled:

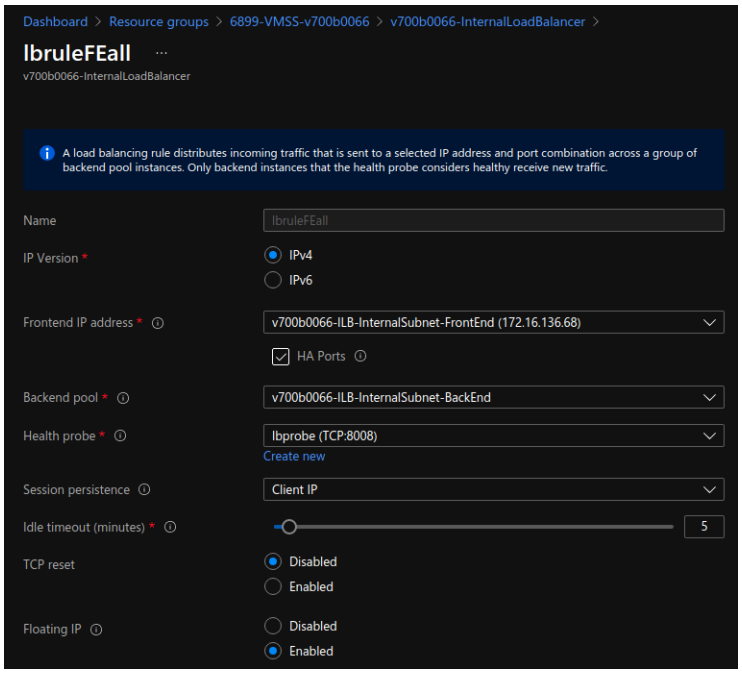
1. In Azure, configure the ELB load balancing rules. Ensure that *Session persistence* is configured to the client IP address and that *Floating IP* is enabled:



2. Configure the ELB outbound rules:



3. Configure the ILB load balancing rules. Ensure that *Session persistence* is configured to the client IP address and that *Floating IP* is enabled:



4. Confirm the configuration in the FortiGate A CLI. The following shows an example of possible output:

```
v700b0066-FGT-A # diagnose ip address list
IP=172.16.136.4->172.16.136.4/255.255.255.192 index=3 devname=port1
IP=172.16.136.69->172.16.136.69/255.255.255.192 index=4 devname=port2
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=7 devname=root
IP=10.255.1.1->10.255.1.1/255.255.255.0 index=11 devname=fortilink
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=12 devname=vsys_ha
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=14 devname=vsys_fgfm

v700b0066-FGT-A #
v700b0066-FGT-A # show system vdom-exception
config system vdom-exception
    edit 10
        set object system.standalone-cluster
    next
end

v700b0066-FGT-A #
v700b0066-FGT-A # show system auto-scale
config system auto-scale
    set status enable
    set role primary
    set sync-interface "port2"
    set psksecret ENC
TJSGPV1J2oxb7+ePiw8Sd42y6fHGYfHm84LeKa2wGTkcMxDfLg94dpuNqB8ID53wke91tNs3lyl0rZ5xc8c
U6NGGLTwS7U3pFkkd0vxCMF37fDVLcItPLDXN2EWXTiX5v2s02QpUTkqIWlAv/KedMpRMuKdx6DDWmhWUoL
nw99CO3zUWQjtf5FAtxIupcL6yGtSAVw==
end
```

```
v700b0066-FGT-A #
v700b0066-FGT-A # show system standalone-cluster
config system standalone-cluster
    config cluster-peer
        edit 1
        set peerip 172.16.136.70
    next
    end
end

v700b0066-FGT-A #
v700b0066-FGT-A # show system ha
config system ha
    set session-pickup enable
    set session-pickup-connectionless enable
    set session-pickup-expectation enable
    set session-pickup-nat enable
    set override disable
end

v700b0066-FGT-A #
v700b0066-FGT-A # show firewall vip 172.16.137.15:22
config firewall vip
    edit "172.16.137.15:22"
        set uuid a26b50cc-db75-51eb-7dd5-a313054c614a
        set extip 20.150.252.91
        set mappedip "172.16.137.15"
        set extintf "port1"
        set portforward enable
        set extport 65022
        set mappedport 22
    next
end

v700b0066-FGT-A #
v700b0066-FGT-A # show firewall vip 172.16.137.15:80
config firewall vip
    edit "172.16.137.15:80"
        set uuid aba58d6a-db75-51eb-118b-b771bfbf59b4
        set extip 20.150.252.91
        set mappedip "172.16.137.15"
        set extintf "port1"
        set portforward enable
        set extport 80
        set mappedport 80
    next
end
```

```
v700b0066-FGT-A #
v700b0066-FGT-A # show firewall vip 172.16.137.15:443
config firewall vip
    edit "172.16.137.15:443"
        set uuid b0e949d8-db75-51eb-fb60-f5537489a0bc
        set extip 20.150.252.91
        set mappedip "172.16.137.15"
        set extintf "port1"
        set portforward enable
        set extport 443
        set mappedport 443
    next
end

v700b0066-FGT-A #
v700b0066-FGT-A # show firewall policy
config firewall policy
    edit 2
        set name "to_VIP"
        set uuid c9ff1fd8-db75-51eb-6b34-e17d224884b9
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "172.16.137.15:22" "172.16.137.15:443" "172.16.137.15:80"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "deep-inspection"
        set av-profile "default"
        set logtraffic all
    next
    edit 3
        set name "to_Internet"
        set uuid d834ffb4-db75-51eb-e370-b6668f0fd24d
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set nat enable
    next
end

v700b0066-FGT-A #
```

```
v700b0066-FGT-A # show router static
config router static
    edit 1
        set gateway 172.16.136.1
        set device "port1"
    next
    edit 2
        set dst 172.16.136.0 255.255.252.0
        set gateway 172.16.136.65
        set device "port2"
    next
    edit 3
        set dst 168.63.129.16 255.255.255.255
        set gateway 172.16.136.65
        set device "port2"
    next
    edit 4
        set dst 168.63.129.16 255.255.255.255
        set gateway 172.16.136.1
        set device "port1"
    next
    edit 137
        set dst 172.16.137.0 255.255.255.0
        set gateway 172.16.136.65
        set device "port2"
    next
end

v700b0066-FGT-A #
v700b0066-FGT-A # get system auto-scale
status              : enable
role                : primary
sync-interface      : port2
primary-ip          : 0.0.0.0
callback-url        :
hb-interval         : 10
psksecret           : *

v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys ha autoscale-peers
Serial#: FGTAZRUPN-GQBR9B
VMID:    9b09d366-f5e2-490f-acab-3bbf2835bd7b
Role:    secondary
IP:      172.16.136.70


v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys ha checksum autoscale-cluster
```

```
================== FGTAZRJ_NNBQZJD0 ==================

is_autoscale_primary()=1
debugzone
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root: 21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all: 92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e

checksum
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root: 21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all: 92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e

================== FGTAZRUPN-GQBR9B ==================

is_autoscale_primary()=0
debugzone
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root: 21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all: 92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e

checksum
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root: 21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all: 92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e

v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session sync
sync_ctx: sync_started=1, sync_tcp=1, sync_others=1,
sync_expectation=1, sync_nat=1, stdalone_sesync=1.
sync: create=115:0, update=505, delete=1:0, query=5
recv: create=7:0, update=22, delete=0:0, query=0
ses pkts: send=0, alloc_fail=0, recv=0, recv_err=0 sz_err=0
udp pkts: send=626, recv=28
nCfg_sess_sync_num=1, mtu=1500, ipsec_tun_sync=1
sync_filter:
       1: vd=-1, szone=0, dzone=0, saddr=0.0.0.0:0.0.0.0, daddr=0.0.0.0:0.0.0.0, sport=0-
65535, dport=0:65535
```

5. Confirm the configuration in the FortiGate B CLI. The following shows an example of possible output:

```
v700b0066-FGT-B # diagnose ip address list
IP=172.16.136.5->172.16.136.5/255.255.255.192 index=3 devname=port1
IP=172.16.136.70->172.16.136.70/255.255.255.192 index=4 devname=port2
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=7 devname=root
IP=10.255.1.1->10.255.1.1/255.255.255.0 index=11 devname=fortilink
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=12 devname=vsys_ha
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=14 devname=vsys_fgfm
```

```
v700b0066-FGT-B #
v700b0066-FGT-B # show system vdom-exception
path=system, objname=vdom-exception, tablename=(null), size=88
config system vdom-exception
    edit 10
        set object system.standalone-cluster
    next
end

v700b0066-FGT-B #
v700b0066-FGT-B # show system auto-scale
path=system, objname=auto-scale, tablename=(null), size=184
config system auto-scale
    set status enable
    set sync-interface "port2"
    set primary-ip 172.16.136.69
    set psksecret ENC
eZcoPrBuiWb56WynxSJPLzPnxnD9SrMSRxHpb8uwW/jFi9tFl+66kj9atAtSlTfoWff/12hQJjp0nECYHWd
/RrUMN0AavBdDFzZM7u8COFk7MgkPmtW+DMJyIojlDS80VGTebNIUES+svJm1wkL7Km4FdNu3xKeZzEzv2V
UoyO1abrdWI50vz0MOOCesK7Xuxq/Kig==
end

v700b0066-FGT-B #
v700b0066-FGT-B # show system standalone-cluster
config system standalone-cluster
    config cluster-peer
        edit 1
        set peerip 172.16.136.69
    next
    end
end

v700b0066-FGT-B #
v700b0066-FGT-B # show system ha
path=system, objname=ha, tablename=(null), size=5960
config system ha
    set session-pickup enable
    set session-pickup-connectionless enable
    set session-pickup-expectation enable
    set session-pickup-nat enable
    set override disable
end

v700b0066-FGT-B #
v700b0066-FGT-B # show firewall vip 172.16.137.15:22
path=firewall, objname=vip, tablename=172.16.137.15:22, size=840
config firewall vip
    edit "172.16.137.15:22"
```

```
        set uuid a26b50cc-db75-51eb-7dd5-a313054c614a
        set extip 20.150.252.91
        set mappedip "172.16.137.15"
        set extintf "port1"
        set portforward enable
        set extport 65022
        set mappedport 22
    next
end

v700b0066-FGT-B #
v700b0066-FGT-B # show firewall vip 172.16.137.15:80
path=firewall, objname=vip, tablename=172.16.137.15:80, size=840
config firewall vip
    edit "172.16.137.15:80"
        set uuid aba58d6a-db75-51eb-118b-b771bfbf59b4
        set extip 20.150.252.91
        set mappedip "172.16.137.15"
        set extintf "port1"
        set portforward enable
        set extport 80
        set mappedport 80
    next
end

v700b0066-FGT-B #
v700b0066-FGT-B # show firewall vip 172.16.137.15:443
path=firewall, objname=vip, tablename=172.16.137.15:443, size=840
config firewall vip
    edit "172.16.137.15:443"
        set uuid b0e949d8-db75-51eb-fb60-f5537489a0bc
        set extip 20.150.252.91
        set mappedip "172.16.137.15"
        set extintf "port1"
        set portforward enable
        set extport 443
        set mappedport 443
    next
end

v700b0066-FGT-B #
v700b0066-FGT-B # show firewall policy
path=firewall, objname=policy, tablename=(null), size=2816
config firewall policy
    edit 2
        set name "to_VIP"
        set uuid c9ff1fd8-db75-51eb-6b34-e17d224884b9
        set srcintf "port1"
```

```
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "172.16.137.15:22" "172.16.137.15:443" "172.16.137.15:80"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "deep-inspection"
        set av-profile "default"
        set logtraffic all
    next
    edit 3
        set name "to_Internet"
        set uuid d834ffb4-db75-51eb-e370-b6668f0fd24d
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set nat enable
    next
end

v700b0066-FGT-B #
v700b0066-FGT-B # show router static
path=router, objname=static, tablename=(null), size=296
config router static
    edit 1
        set gateway 172.16.136.1
        set device "port1"
    next
    edit 2
        set dst 172.16.136.0 255.255.252.0
        set gateway 172.16.136.65
        set device "port2"
    next
    edit 3
        set dst 168.63.129.16 255.255.255.255
        set gateway 172.16.136.65
        set device "port2"
    next
    edit 4
        set dst 168.63.129.16 255.255.255.255
        set gateway 172.16.136.1
        set device "port1"
```

```
    next
    edit 137
        set dst 172.16.137.0 255.255.255.0
        set gateway 172.16.136.65
        set device "port2"
    next
end

v700b0066-FGT-B #
v700b0066-FGT-B # get system auto-scale
path=system, objname=auto-scale, tablename=(null), size=184
status              : enable
role                : secondary
sync-interface      : port2
primary-ip          : 172.16.136.69
callback-url        :
hb-interval         : 10
psksecret           : *

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys ha autoscale-peers
Serial#: FGTAZRJ_NNBQZJD0
VMID:    d00cd4bc-2d8f-4fb5-a42f-0297d5e52db7
Role:    primary
IP:      172.16.136.69


v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys ha checksum autoscale-cluster

================== FGTAZRUPN-GQBR9B ==================

is_autoscale_primary()=0
debugzone
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root: 21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all: 92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e

checksum
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root: 21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all: 92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e

================== FGTAZRJ_NNBQZJD0 ==================

is_autoscale_primary()=1
debugzone
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
```

```
root: 21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all: 92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e

checksum
global: b7 0b d4 ae bd 33 00 2d 81 e5 b4 77 79 06 41 8d
root: 21 41 b7 00 7c 7e 66 86 26 99 be 0b 92 88 ed 1e
all: 92 7d d2 09 b2 56 a2 86 9a 23 f5 72 d0 90 c3 1e

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session sync
sync_ctx: sync_started=1, sync_tcp=1, sync_others=1,
sync_expectation=1, sync_nat=1, stdalone_sesync=1.
sync: create=59:0, update=219, delete=0:0, query=6
recv: create=11:0, update=45, delete=0:0, query=0
ses pkts: send=0, alloc_fail=0, recv=0, recv_err=0 sz_err=0
udp pkts: send=284, recv=51
nCfg_sess_sync_num=1, mtu=1500, ipsec_tun_sync=1
sync_filter:
       1: vd=-1, szone=0, dzone=0, saddr=0.0.0.0:0.0.0.0, daddr=0.0.0.0:0.0.0.0, sport=0-
65535, dport=0:65535

v700b0066-FGT-B #
```

When autoscaling is enabled, the configuration syncs between the primary FortiGate to the secondary FortiGate in the virtual machine scale set (VMSS). With FGSP configured, sessions sync to all VMSS members. With the ELB performing DNAT and the firewall VIP policy configured on the FortiGate, original client IP addresses are kept.

```
fosqa@pc15:~$ w
 16:26:02 up 38 days,  1:29,  3 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
packet   pts/0    13.83.82.124     Wed15   23:45m  0.02s  0.00s tail -f /var/lo
fosqa    pts/1    207.102.138.19   Wed15    2.00s  0.03s  0.00s w
fosqa    pts/3    13.66.229.197    Wed15   23:45m  0.02s  0.00s tail -f /var/lo
fosqa@pc15:~$
fosqa@pc15:~$ tail /var/log/nginx/access.log
165.22.97.76 - - [12/Aug/2021:15:55:11 -0700] "GET /stalker_portal/c/version.js HTTP/1.1"
444 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/74.0.3729.169 Safari/537.36"
165.22.97.76 - - [12/Aug/2021:15:55:11 -0700] "GET /stream/live.php HTTP/1.1" 444 0 "-"
"Roku/DVP-9.10 (289.10E04111A)"
165.22.97.76 - - [12/Aug/2021:15:55:12 -0700] "GET /flu/403.html HTTP/1.1" 444 0 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/74.0.3729.169 Safari/537.36"
117.193.32.121 - - [12/Aug/2021:15:56:15 -0700] "GET / HTTP/1.1" 444 0 "-" "-"
88.2.174.20 - - [12/Aug/2021:16:04:30 -0700] "GET / HTTP/1.1" 200 443 "-" "Mozilla/5.0
(Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2
Safari/601.7.7"
45.79.155.112 - - [12/Aug/2021:16:13:23 -0700] "GET / HTTP/1.1" 200 299 "-" "Mozilla/5.0
(Windows NT 6.1; WOW64; rv:8.0) Gecko/20100101 Firefox/8.0"
117.223.219.238 - - [12/Aug/2021:16:14:14 -0700] "GET / HTTP/1.1" 444 0 "-" "-"
59.95.127.92 - - [12/Aug/2021:16:16:03 -0700] "GET / HTTP/1.1" 444 0 "-" "-"
103.197.205.191 - - [12/Aug/2021:16:16:28 -0700] "GET / HTTP/1.1" 444 0 "-" "-"
128.199.23.44 - - [12/Aug/2021:16:21:03 -0700] "GET / HTTP/1.1" 200 299 "-" "Mozilla/5.0
(Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.78
```

```
Safari/537.36 OPR/47.0.2631.39"
fosqa@pc15:~$
```

For example, when multiple uses are connecting to PC15 via SSH from the Internet, DNAT sessions sync between the FortiGates:

```
v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session filter clear

v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session filter proto 6

v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session filter dport 65022

v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session clear

v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session list
total session 0

v700b0066-FGT-A #
v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session list

session info: proto=6 proto_state=11 duration=9 expire=3595 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty synced f00
statistic(bytes/packets/allow_err): org=4305/22/1 reply=4533/19/1 tuples=3
tx speed(Bps/kbps): 436/3 rx speed(Bps/kbps): 459/3
orgin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=172.16.136.65/172.16.136.1
hook=pre dir=org act=dnat 207.102.138.19:57402->20.150.252.91:65022(172.16.137.15:22)
hook=post dir=reply act=snat 172.16.137.15:22->207.102.138.19:57402(20.150.252.91:65022)
hook=post dir=org act=noop 207.102.138.19:57402->172.16.137.15:22(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0
serial=00001fd4 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdb_link_id=00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x001008

session info: proto=6 proto_state=11 duration=10 expire=3589 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr f00 syn_ses
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=dnat 13.83.82.124:55212->20.150.252.91:65022(172.16.137.15:22)
```

```
hook=post dir=reply act=snat 172.16.137.15:22->13.83.82.124:55212(20.150.252.91:65022)
hook=post dir=org act=noop 13.83.82.124:55212->172.16.137.15:22(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0
serial=00000591 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdb_link_id=00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x001000
total session 2

v700b0066-FGT-A #
v700b0066-FGT-A #
v700b0066-FGT-A # diagnose sys session sync
sync_ctx: sync_started=1, sync_tcp=1, sync_others=1,
sync_expectation=1, sync_nat=1, stdalone_sesync=1.
sync: create=213:0, update=899, delete=2:0, query=11
recv: create=32:0, update=119, delete=1:0, query=1
ses pkts: send=0, alloc_fail=0, recv=0, recv_err=0 sz_err=0
udp pkts: send=1125, recv=152
nCfg_sess_sync_num=1, mtu=1500, ipsec_tun_sync=1
sync_filter:
       1: vd=-1, szone=0, dzone=0, saddr=0.0.0.0:0.0.0.0, daddr=0.0.0.0:0.0.0.0, sport=0-65535,
dport=0:65535

v700b0066-FGT-A #
```

```
v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session filter clear

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session filter proto 6

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session filter dport 65022

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session clear

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session list
total session 0

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session list

session info: proto=6 proto_state=11 duration=12 expire=3587 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr f00 syn_ses
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=dnat 207.102.138.19:57402->20.150.252.91:65022(172.16.137.15:22)
hook=post dir=reply act=snat 172.16.137.15:22->207.102.138.19:57402(20.150.252.91:65022)
```

```
hook=post dir=org act=noop 207.102.138.19:57402->172.16.137.15:22(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0
serial=00001fd4 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdb_link_id=00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x001000

session info: proto=6 proto_state=11 duration=13 expire=3598 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty synced f00
statistic(bytes/packets/allow_err): org=3861/27/1 reply=3965/21/1 tuples=3
tx speed(Bps/kbps): 277/2 rx speed(Bps/kbps): 284/2
orgin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=172.16.136.65/172.16.136.1
hook=pre dir=org act=dnat 13.83.82.124:55212->20.150.252.91:65022(172.16.137.15:22)
hook=post dir=reply act=snat 172.16.137.15:22->13.83.82.124:55212(20.150.252.91:65022)
hook=post dir=org act=noop 13.83.82.124:55212->172.16.137.15:22(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0
serial=00000591 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdb_link_id=00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x001008
total session 2

v700b0066-FGT-B #
v700b0066-FGT-B # diagnose sys session sync
sync_ctx: sync_started=1, sync_tcp=1, sync_others=1,
sync_expectation=1, sync_nat=1, stdalone_sesync=1.
sync: create=23:0, update=89, delete=1:0, query=1
recv: create=43:0, update=146, delete=0:0, query=3
ses pkts: send=0, alloc_fail=0, recv=0, recv_err=0 sz_err=0
udp pkts: send=114, recv=187
nCfg_sess_sync_num=1, mtu=1500, ipsec_tun_sync=1
sync_filter:
       1: vd=-1, szone=0, dzone=0, saddr=0.0.0.0:0.0.0.0, daddr=0.0.0.0:0.0.0.0, sport=0-65535,
dport=0:65535

v700b0066-FGT-B #
```

Troubleshooting

Determining the FortiGate Autoscale release version

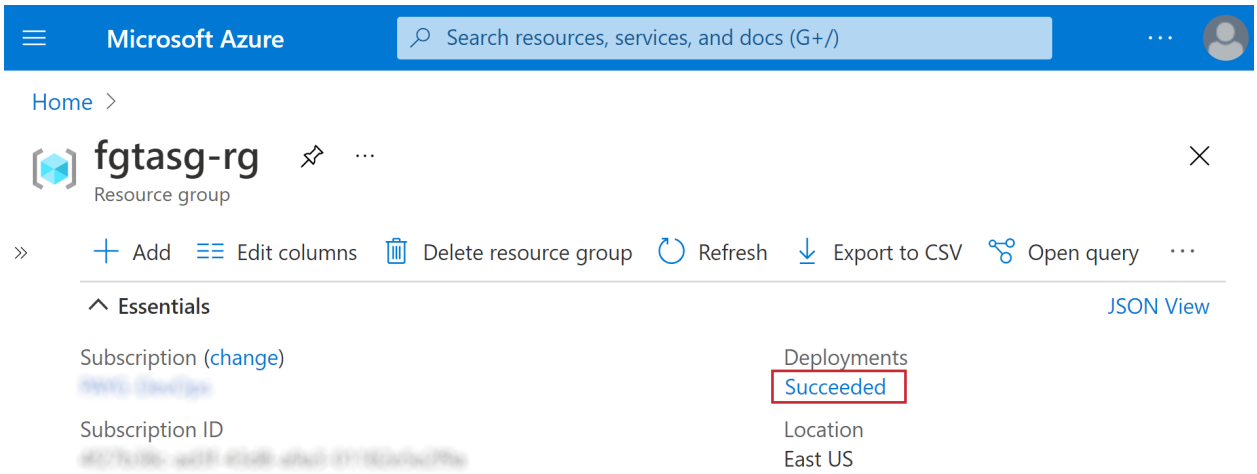
To determine the release version of a deployment, navigate to the *Microsoft.Template Outputs* by following the steps in Locating deployment Outputs on page 102. The release version is in the `deploymentPackageVersion`.

Election of the primary FortiGate was not successful

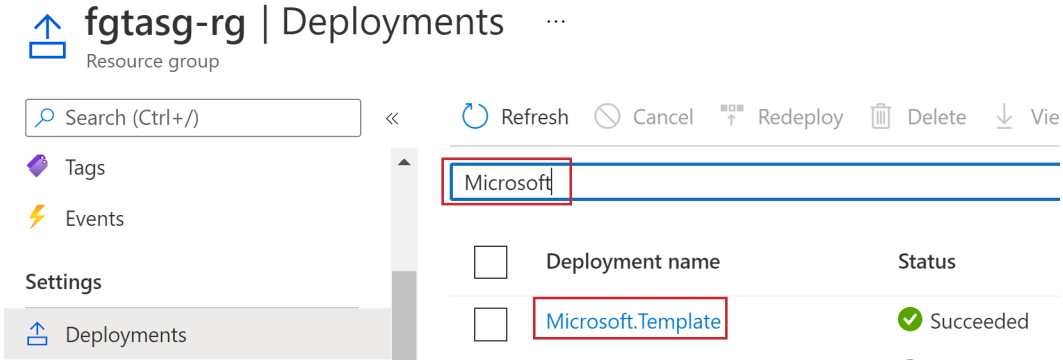
If the election of the primary FortiGate is not successful, reset the elected primary FortiGate. If the reset does not solve the problem, please contact support.

Locating deployment Outputs

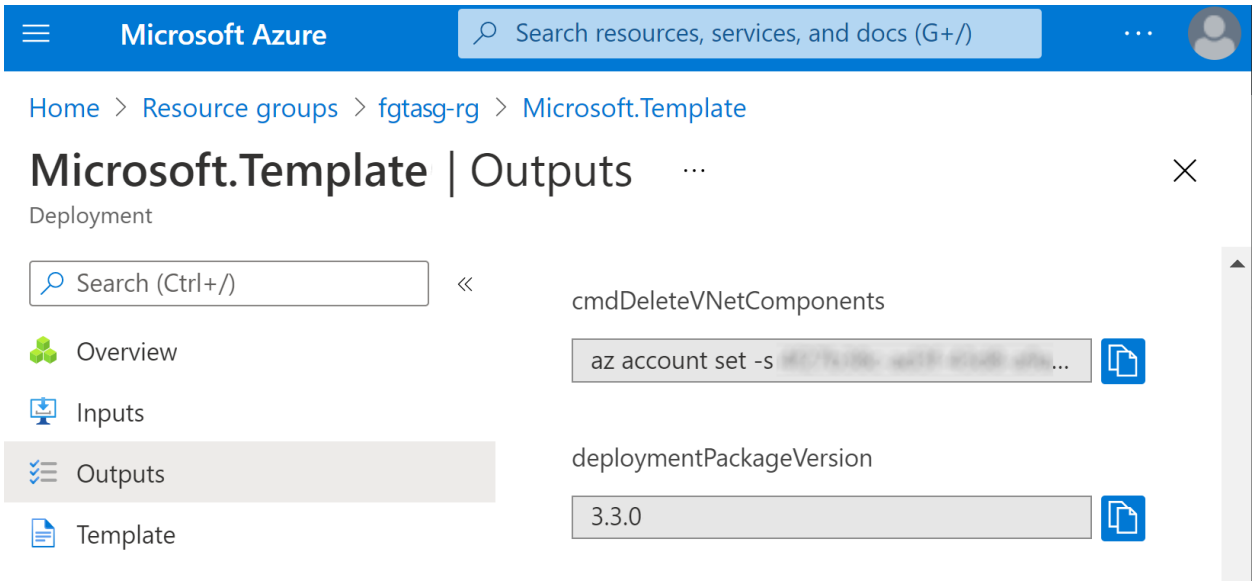
1. Load the resource group *Overview* page. For details, refer to the section To load a resource group: on page 74.
2. Click the link under *Deployments*.



3. From the *Deployments* page, click the *Microsoft.Template*.



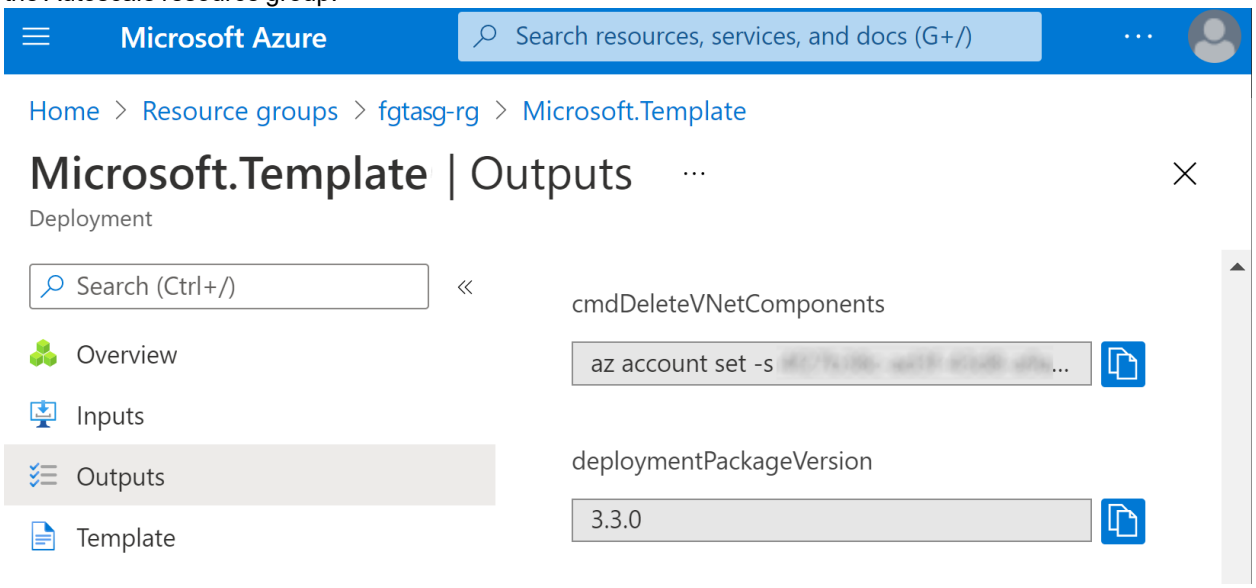
4. In the navigation column, click *Outputs*.



Redeploying with an existing VNet fails

Prior to redeploying with your existing VNet, you must ensure that the VNet meets the Requirements when using an existing VNet on page 60. You must also perform a VNet related cleanup using the following steps:

1. Load the deployment Outputs for the VNet resource group. If your deployment only has one resource group, this is the Autoscale resource group.



2. Copy the value of `cmdDeleteVNetComponents` and run it as an Azure CLI command (click >_ to launch the CLI) to perform the required cleanup.
3. If your deployment has two resource groups, delete the Autoscale resource group. Otherwise, delete the following components:
   - Azure Cosmos DB account
   - App Service

- Application Insights (if present)
- App Service plan
- Storage account

4. Delete the following components from the VNet resource group:
   - the Public Load balancer
   - the Internal Load balancer
   - the Virtual machine scale set for BYOL
   - the Virtual machine scale set for PAYG
   - the Public IP address (if created by the autoscale deployment and you don't want to reuse it)

Resetting the elected primary FortiGate

To reset the elected primary FortiGate, navigate to the CosmosDB *FortiGateAutoscale* and open the table *FortiGatePrimaryElection* and delete the only item in the table.

A new primary FortiGate will be elected and a new record will be created as a result.

For details on locating the CosmosDB *FortiGateAutoscale* and the table *FortiGatePrimaryElection*, refer to the section Verifying the deployment on page 74.

Stack has stopped working

If the stack stops working when it previously used to work, look up the Function App *Additional Outbound IP Addresses* and ensure that each listed IP address has a corresponding entry in the Cosmos DB firewall. Any IP address not listed in the Cosmos DB firewall will be blocked, thus causing the Autoscale function to be blocked.

For details on how the Cosmos DB firewall is configured, refer to the section Security features for network communication on page 78.

For details on when Function App outbound IP addresses change, refer to the Microsoft article When outbound IPs change.

Troubleshooting using Application Insights

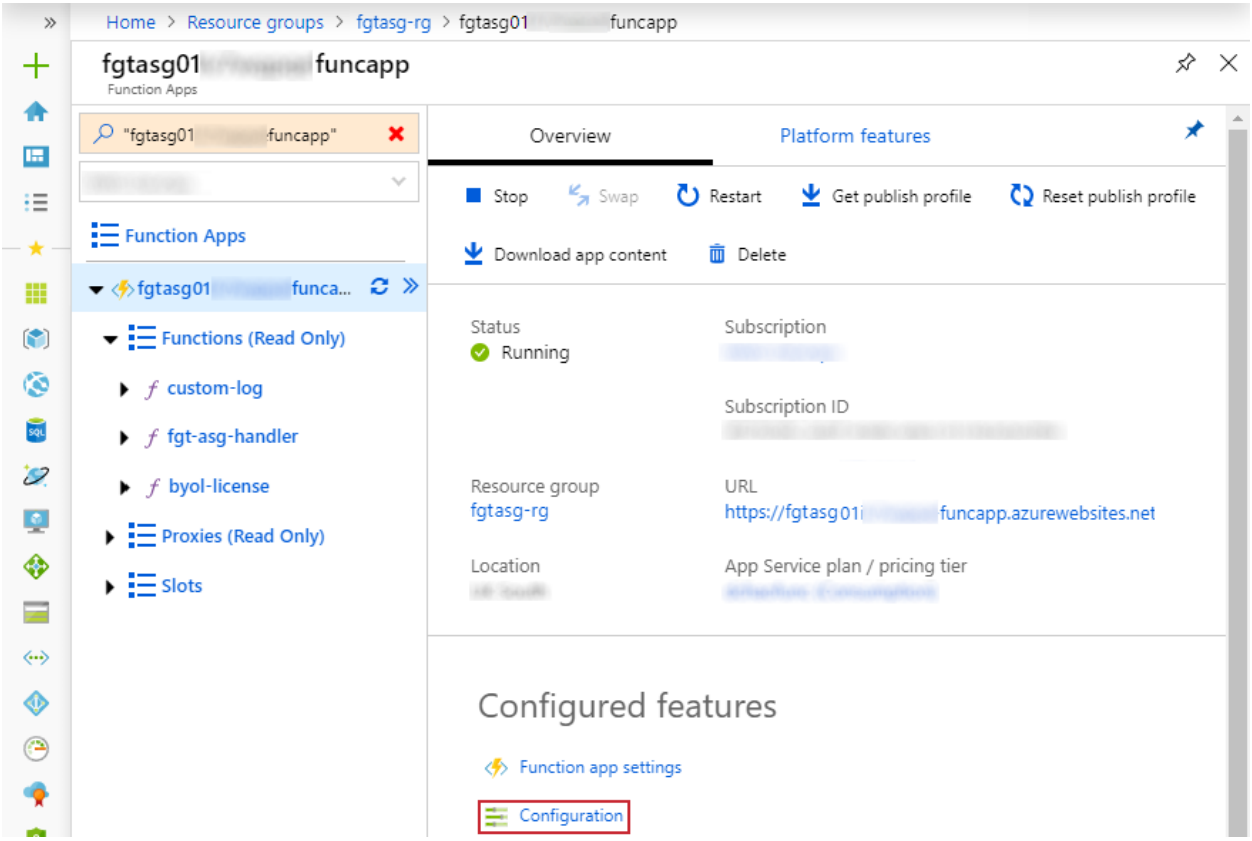
Application Insights can help you troubleshoot the deployment. It is automatically enabled if your region supports it.

Troubleshooting using environment variables

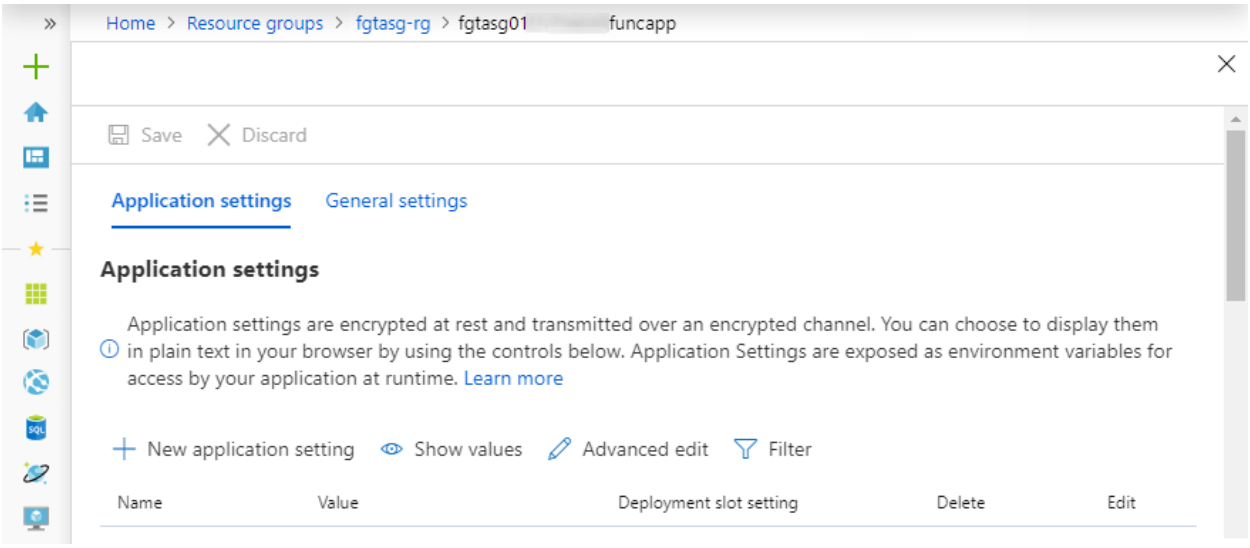
Environment variables are available to assist in troubleshooting the current FortiGate Autoscale deployment. These variables and details on how to use them are listed in the section Troubleshooting environment variables on page 108

1. Load the Function App. For detailed steps, refer to the Function App portion of the section Verifying the deployment on page 74.

2. Under *Configured features*, click *Configuration* .



3. Edit settings as needed.



Changing environment variables other than the troubleshooting ones can cause unexpected behavior. Modify them at your own risk.

Appendix

FortiGate Autoscale for Azure features

Major components

- *The Function App*. The Function App handles all the autoscaling features including: primary/secondary role assignment, license distribution, and failover management.
- *The BYOL Scale Set*. This scale set contains 0 to many FortiGate-VMs of the BYOL licensing model and is a VMSS with a fixed size. Users can set the size to match the number of valid licenses they own. Licenses can be purchased from FortiCare.

  For BYOL-only and hybrid licensing deployments, the *BYOL instance Count* must be at least 2. These FortiGate-VMs are the main instances and are fixed and running 7x24. If it is set to 1 and the instance fails to work, the current FortiGate-VM configuration will be lost.

- *The PAYG Scale Set*. The Scale Set contains 0 to many FortiGate-VMs of the PAYG licensing model and will dynamically scale-out or scale-in based on the scaling metrics specified by the parameters *Scale Out Threshold* and *Scale in Threshold*.

  For PAYG-only deployments, the *PAYG instance Count* must be at least 2. These FortiGate-VMs are the main instances and are fixed and running 7x24. If it is set to 1 and the instance fails to work, the current FortiGate-VM configuration will be lost.

- *The Blob Containers*.
  - The *configset* container contains files that are loaded as the initial configuration of a new FortiGate-VM instance.
    - *baseconfig* is the base configuration. This file can be modified as needed to meet your network requirements. Placeholders such as {SYNC_INTERFACE} are explained in the Configset placeholders on page 107 table below.
    - *httproutingpolicy* and *httpsroutingpolicy* are provided as part of the base configset - for a common use case - and specify the FortiGate firewall policy for VIPs for *http* routing and *https* routing respectively. This common use case includes a VIP on port 80 and a VIP on port 443 with a policy that points to an internal load balancer.
    - *extrastaticroute* is empty by default. Configurations for static routes can be added if they are needed in a network. An example of manually adding a static route:

      ```
      # config router static
         edit 1
            set dst 168.63.129.16 255.255.255.255
            set gateway <subnet gateway>
            set priority <any number>
            set device "<port name>"
         next
      end
      ```
  - The *fgt-asg-license* container contains the BYOL license files.

- *Database tables*. These tables are required to store information such as health check monitoring, primary election, state transitions, etc. These records should not be modified unless required for troubleshooting purposes.
- *Networking Components*.
  - One virtual network
  - Two Load Balancers (with names ending with *-external-load-balancer* and *-internal-load-balancer*)
  - One network security group (with a name ending with *-network-security-group*)
  - One public IP address
  - Four route tables

Configset placeholders

When the FortiGate-VM requests the configuration from the Autoscaling handler function, the placeholders in the table below will be replaced with actual values for the Autoscaling group.

Placeholder	Type	Description
{SYNC_ INTERFACE}	Text	The interface for FortiGate-VMs to synchronize information. Specify as port1, port2, port3, etc. All characters must be lowercase.
{CALLBACK_URL}	URL	The full URL of the Autoscaling handler function.
{PSK_SECRET}	Text	The Pre-Shared Key used in FortiOS.
{ADMIN_PORT}	Number	The admin port will be replaced with 443.
{HEART_BEAT_ INTERVAL}	Number	The time interval (in seconds) that the FortiGate-VM waits between sending heartbeat requests to the Autoscale handler function. This placeholder is only in the hybrid licensing deployment.

Function App environment variables

Azure infrastructure related environment variables

The variables in the table below hold information that enables the function to use the required Azure services. Changing their values may cause services to be unreachable by the function. Modify them at your own risk.

Variable name	Description
RESOURCE_GROUP	Name of the resource group where the template is deployed in.
CLIENT_ID	Descriptions of these variables are identical to those of the related parameters which are described in the section Configurable variables on page 66. • REST_APP_ID: *Service Principal App ID on page 70* • REST_APP_SECRET: *Service Principal App Secret on page 70* • WEBSITE_RUN_FROM_ZIP: *Package Res URL on page 69*
CLIENT_SECRET	
WEBSITE_RUN_FROM_ZIP	
AUTOSCALE_DB_PRIMARY_ KEY	This is the CosmosDB account access key automatically created with the CosmosDB account.

Variable name	Description
TENANT_ID	The Azure Directory ID for the Active Directory of your current subscription.
SUBSCRIPTION_ID	Your Azure Subscription ID.
AUTOSCALE_DB_ACCOUNT	The CosmosDB account created for the current FortiGate Autoscale deployment.
AZURE_STORAGE_ACCOUNT	This is the Blob Storage account name automatically created during the deployment.
AZURE_STORAGE_ACCESS_KEY	This is the Blob Storage account access key automatically created with the Blob Storage account.

FortiGate Autoscale required environment variables

Changing the values of the following variables can cause unexpected function behavior. Modify them at your own risk.

Variable name	Description
UNIQUE_ID	Reserved, empty string.
CUSTOM_ID	Reserved, empty string.
RESOURCE_TAG_PREFIX	An Autoscaling feature variable that is automatically created. Reserved for future use.
AUTOSCALE_KEY_VAULT_NAME	Name of the Key Vault service.

Troubleshooting environment variables

The following variables assist in troubleshooting the current FortiGate Autoscale deployment.

Variable name	Description
DEBUG_SAVE_CUSTOM_LOG	Set to *true* to save script logs to the DB table *CUSTOM_LOG*. This is the default behavior. Set to *false* to disable this feature.
DEBUG_LOGGER_OUTPUT_QUEUE_ENABLED	Set to *true* to concatenate all log output into one (1) log item in the Azure logging system. Set to *false* for every log output to have its own log item in the Azure logging system. This is the default behavior.
DEBUG_LOGGER_TIMEZONE_OFFSET	Set to the UTC offset of the current deployment location for a better logging display time.

For details on how to modify the troubleshooting environment variables, refer to the section Troubleshooting using environment variables on page 104.

Replacing the FortiAnalyzer

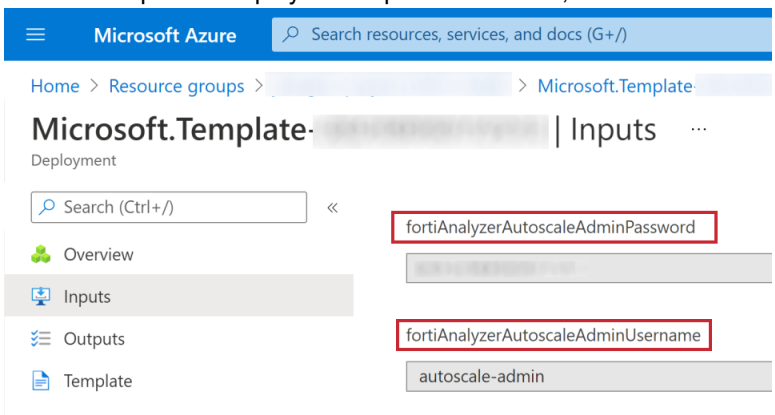
To replace the FortiAnalyzer:

1. Create a new FortiAnalyzer resource in Azure in a location accessible by the FortiGate-VM in Subnet 1.
2. Upload a valid license for the FortiAnalyzer. For details on how to do so, refer to the section Uploading files to the Storage account on page 72.
3. Log in into the FortiAnalyzer-VM.
4. (Optional) Restore a configuration from a backup.
5. If necessary, create an admin user for FortiGate Autoscale to use. To retrieve the ones from the initial deployment, refer to the section Retrieving the FortiAnalyzer administrator username and password on page 109.
6. Update the FortiAnalyzer public IP address resource by first dissociating the public IP address from the previous FortiAnalyzer and then associating the public IP address with the new FortiAnalyzer.
7. If it is necessary to replace the public IP address, you will need to:
   a. Locate the Settings item with key: *faz-ip*. For details, refer to the section Modifying the Autoscale settings in Cosmos DB on page 82.
   b. Update the value to the new public IP address.
   c. Wait up to 60 seconds for the change to become effective.

Retrieving the FortiAnalyzer administrator username and password

During the initial deployment, these were specified in the template parameters *FortiAnalyzer Autoscale Admin Username* and *FortiAnalyzer Autoscale Admin Password*. These values can be retrieved after deployment using each of these methods:

- Look them up in the deployment Inputs. For details, refer to the section Locating deployment Outputs on page 102.



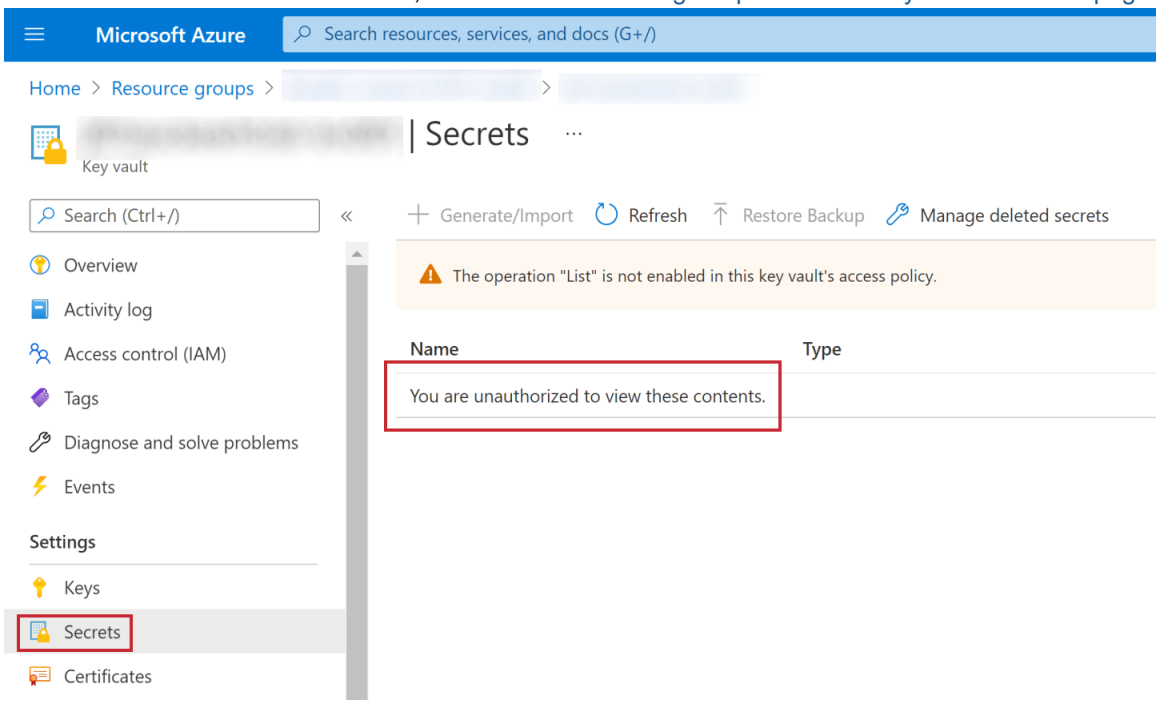
- Use the FortiAnalyzer CLI commands:
  ```
  config system admin user
  show
  ```
  The first line of the output contains the *FortiAnalyzer Autoscale Admin Username*.
- Retrieve them from *Key Vault* > *secrets*. The *FortiAnalyzer Autoscale Admin Username* is stored as *faz-autoscale-admin-username*. For details, refer to the section Viewing and modifying secrets in the Key vault on page 109.

Viewing and modifying secrets in the Key vault

The first time you load the Key vault Secrets, you may need to grant permissions to your account.

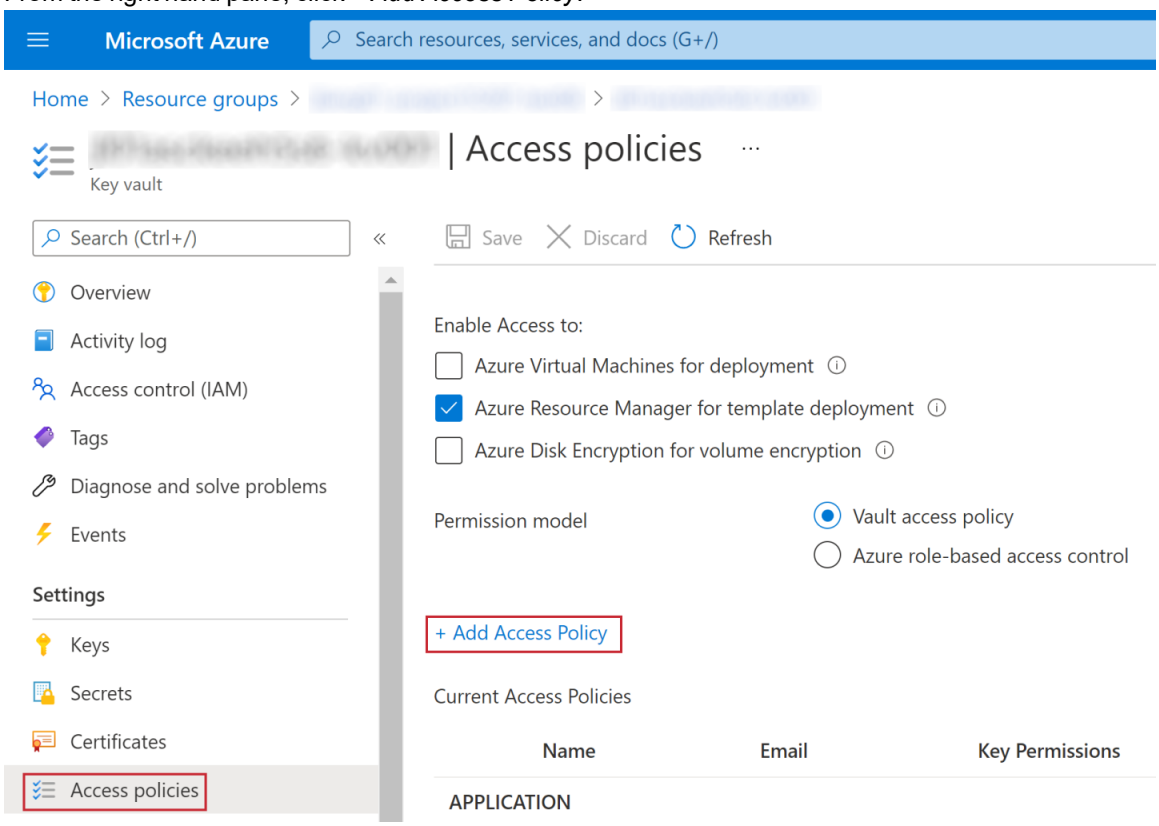
To locate the Key vault secrets:

1. Load the Autoscale resource group. For details, refer to the section To load a resource group: on page 74.
2. Click the name of the item of type *Key vault*.
3. From the navigation column, under *Settings*, select *Secrets*.
4. If the warning “You are unauthorized to view these contents” is displayed, you will need to grant permissions to your account. For details on how to do this, refer to the section To grant permissions to your account: on page 111.

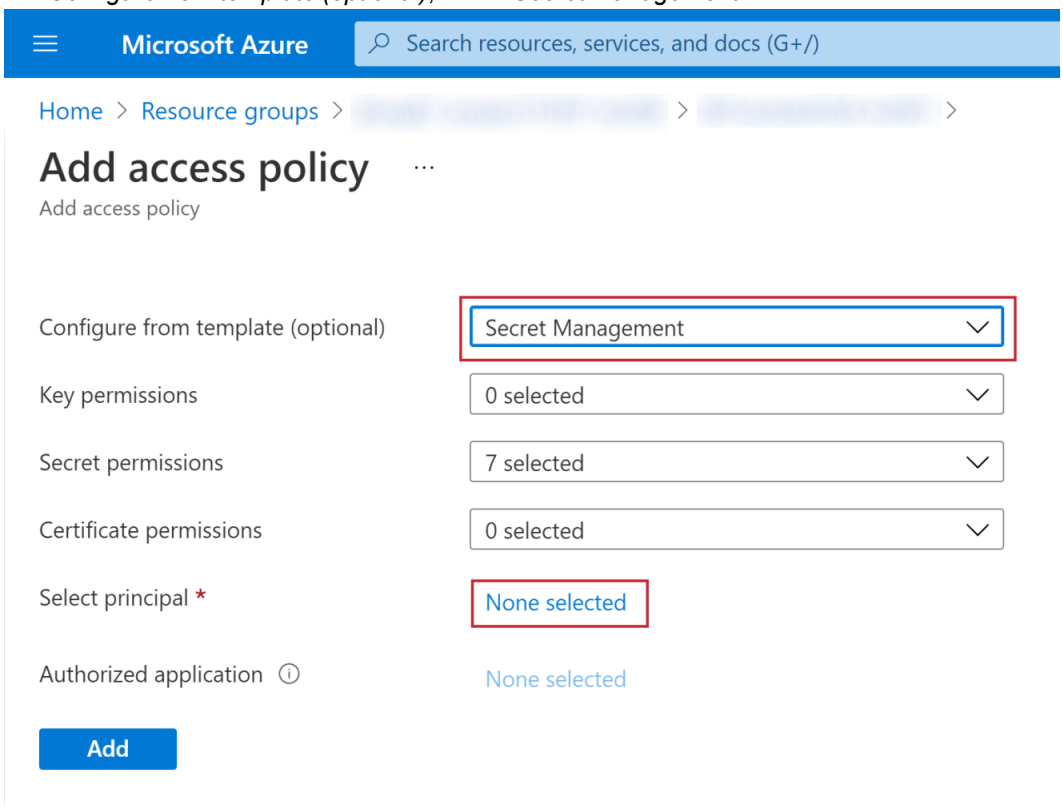


To grant permissions to your account:

1. From the navigation column, under *Settings*, select *Access Policies.*
2. From the right hand pane, click *+ Add Access Policy*.



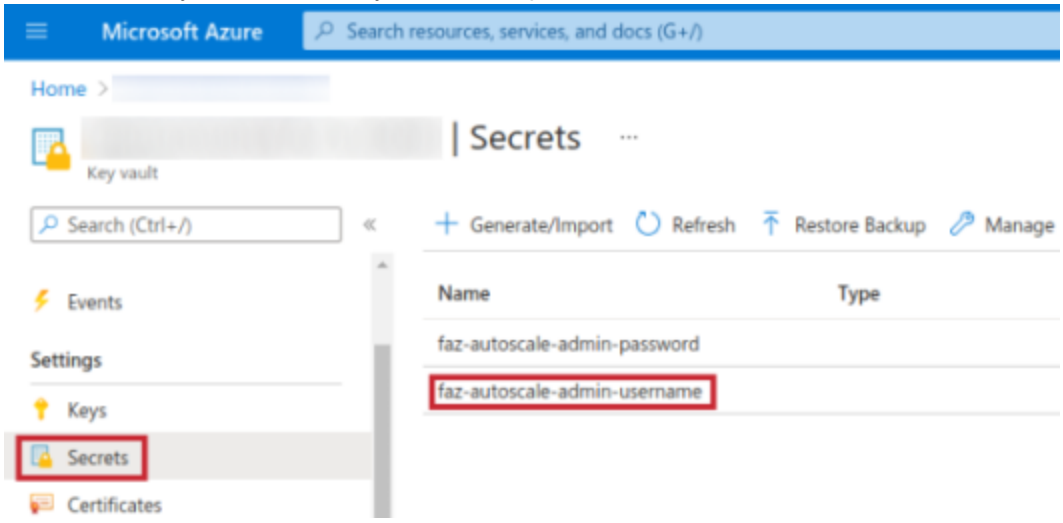
3. For *Configure from template (optional)*, select *Secret Management*.



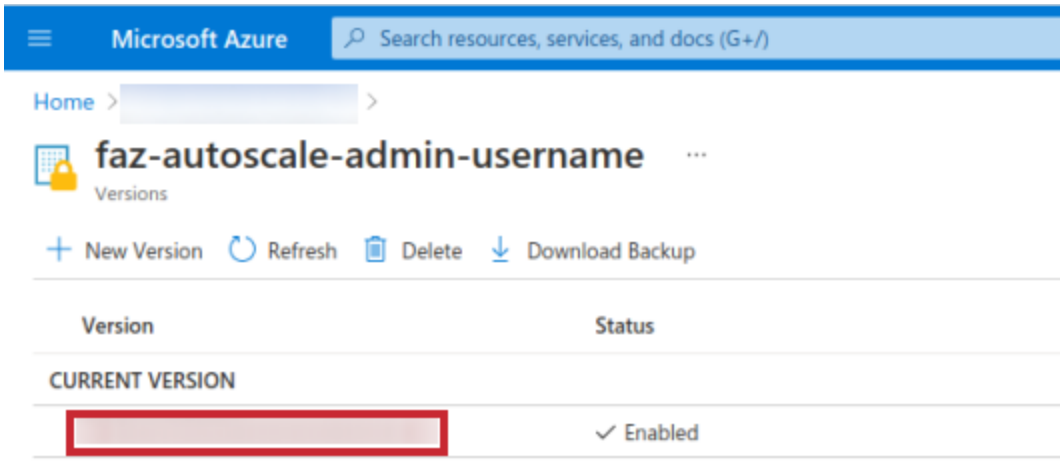
4. For *Select principal **, click *None selected* and choose your account.
5. Leave the *Authorized application* as is.
6. Click *Add*.
7. Click *Save* to apply the changes of granting your account permissions to the Secrets.

To view a stored secret:

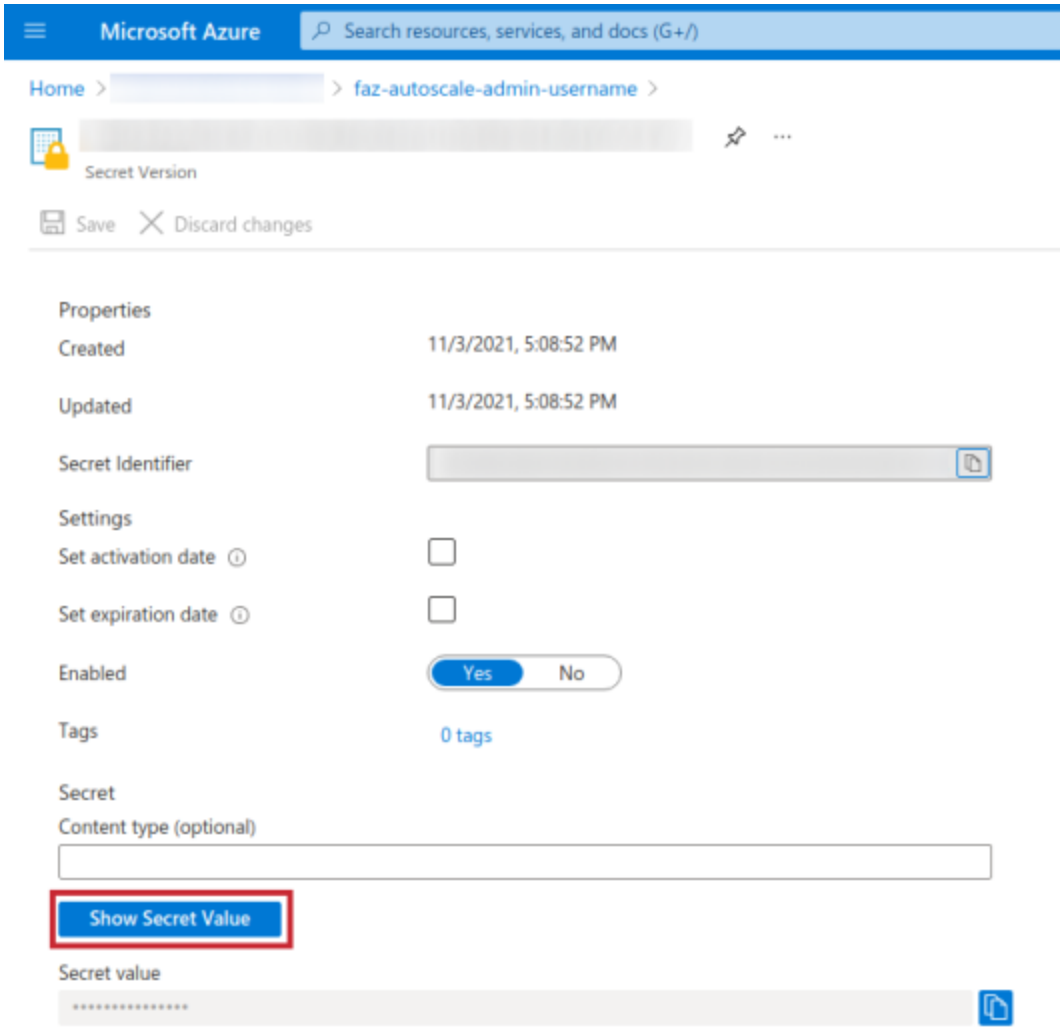
1. Click the secret you want to modify. In the example below, *faz-autoscale-admin-username* is selected.



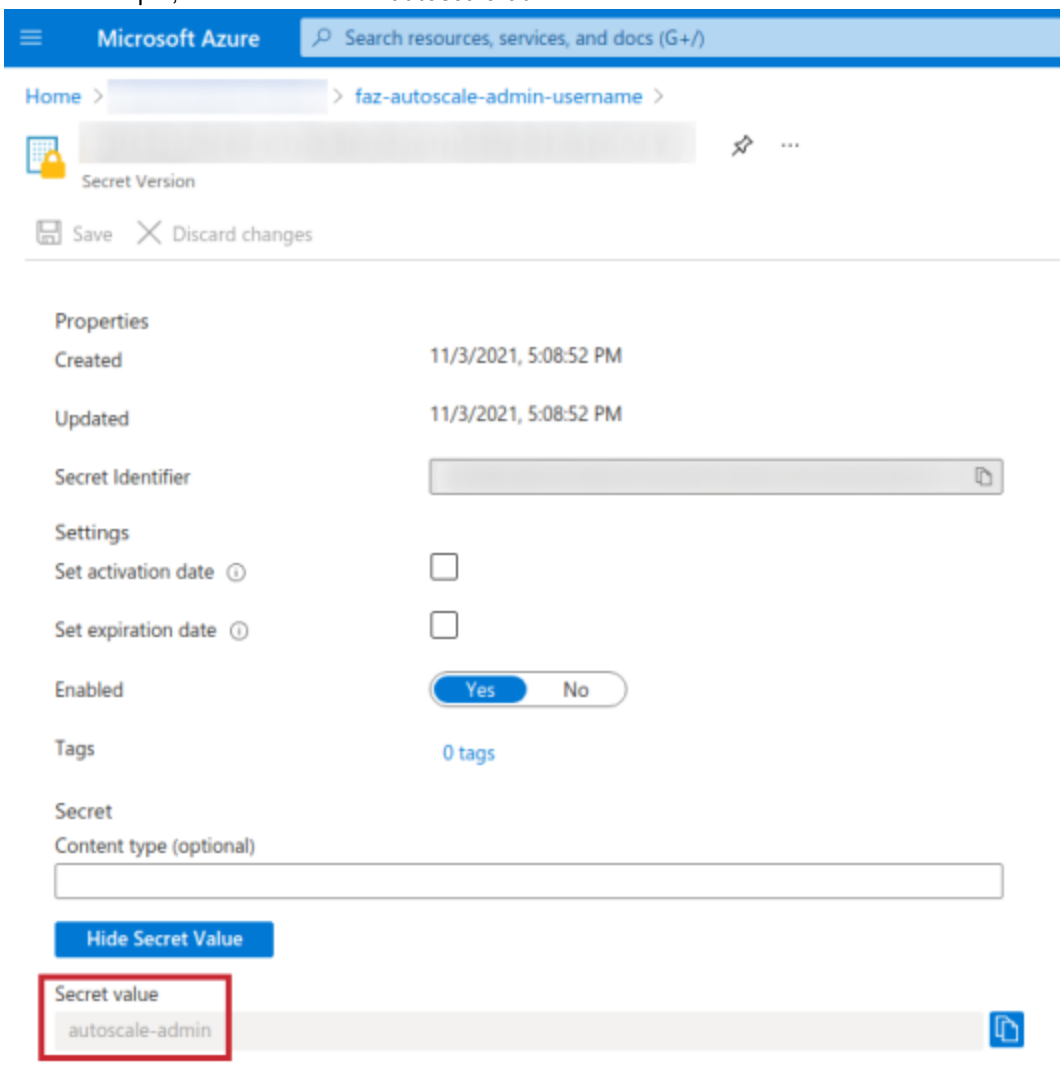
2. Click the item under *CURRENT VERSION*.



3. Click *Show Secret Value*.

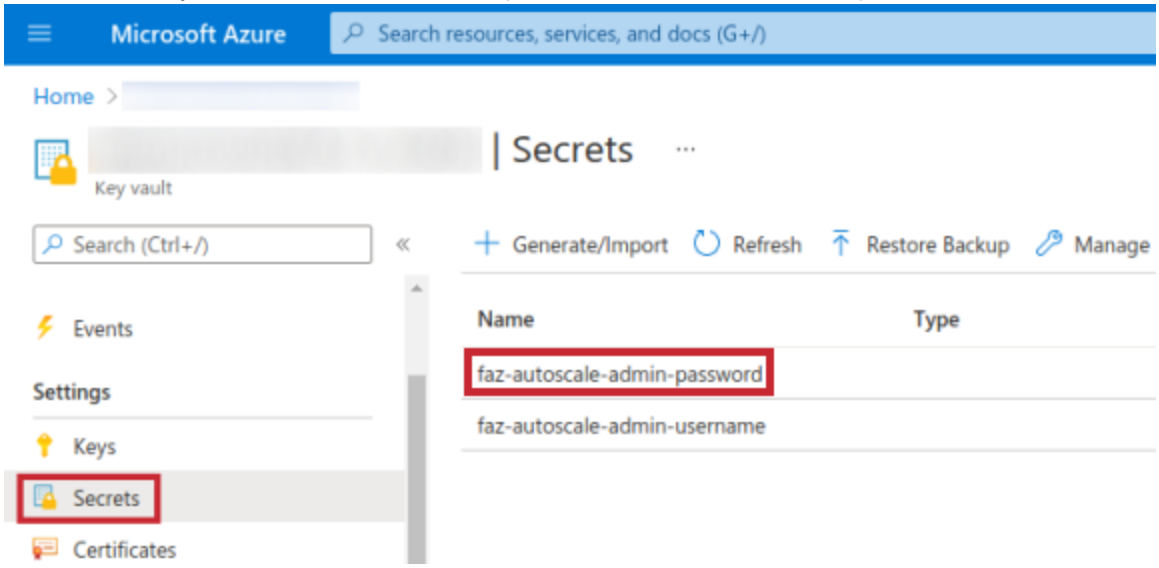


4. In this example, the secret value is *autoscale-admin*.

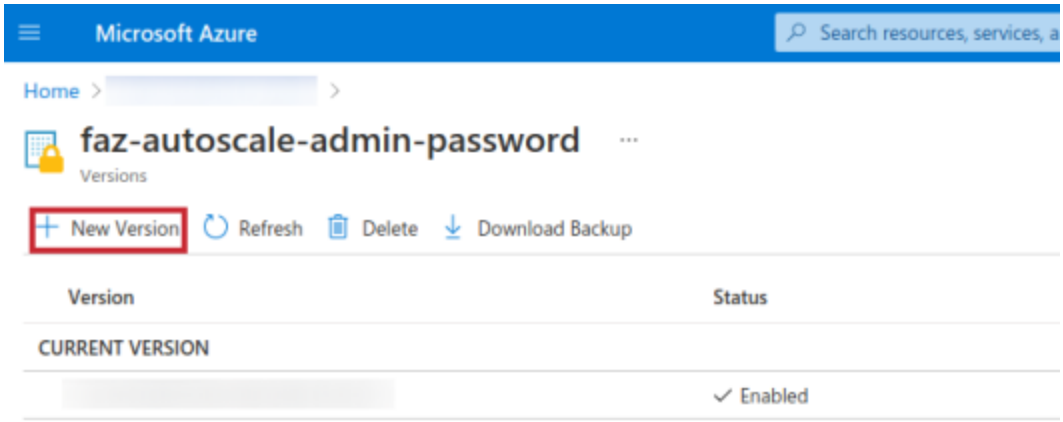


To modify a secret:

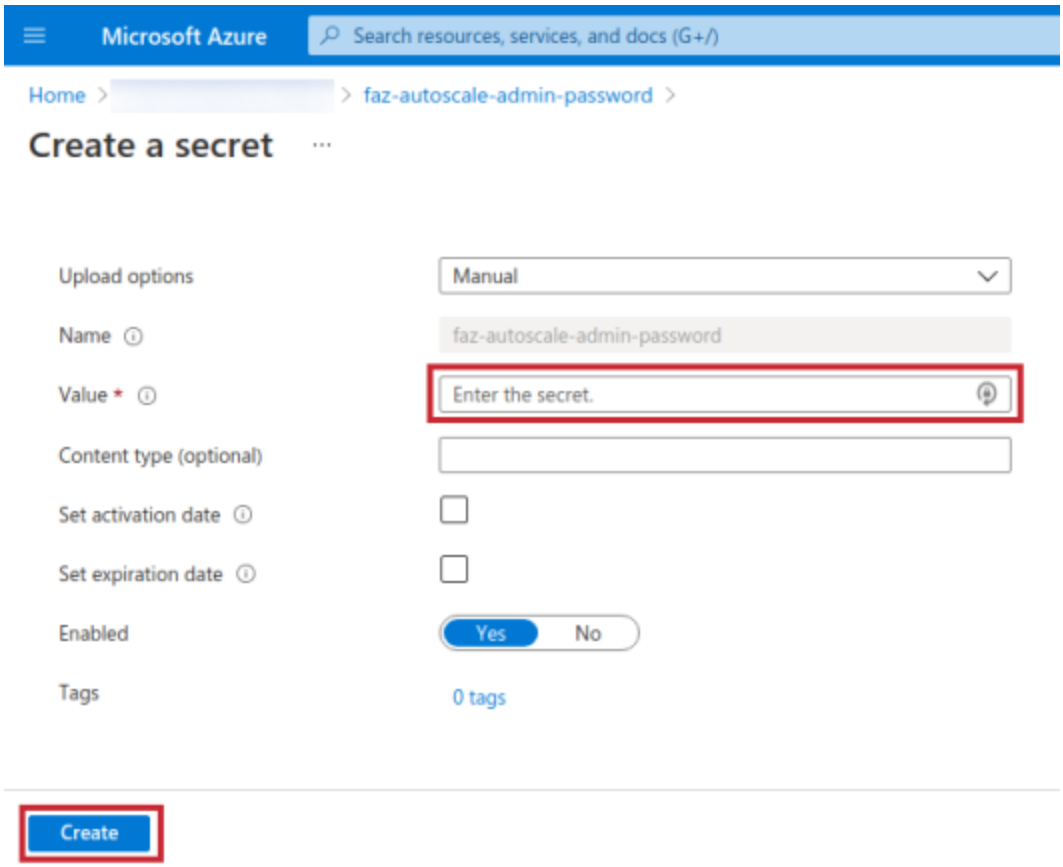
1. Click the secret you want to view. In the example below, *faz-autoscale-admin-password* is selected.



2. Click *+ New Version*.



3. Enter the new secret in the *Value* * field and then click *Create*.



Cloud-init

In Auto Scaling, a FortiGate uses the `cloud-init` feature to pre-configure the instances when they first come up. During template deployment, an internal API Gateway endpoint will be created.

A FortiGate sends requests to the endpoint to retrieve necessary configuration after initialization.

Use this FOS CLI command to display information for your devices:

```
# diagnose debug cloudinit show
```

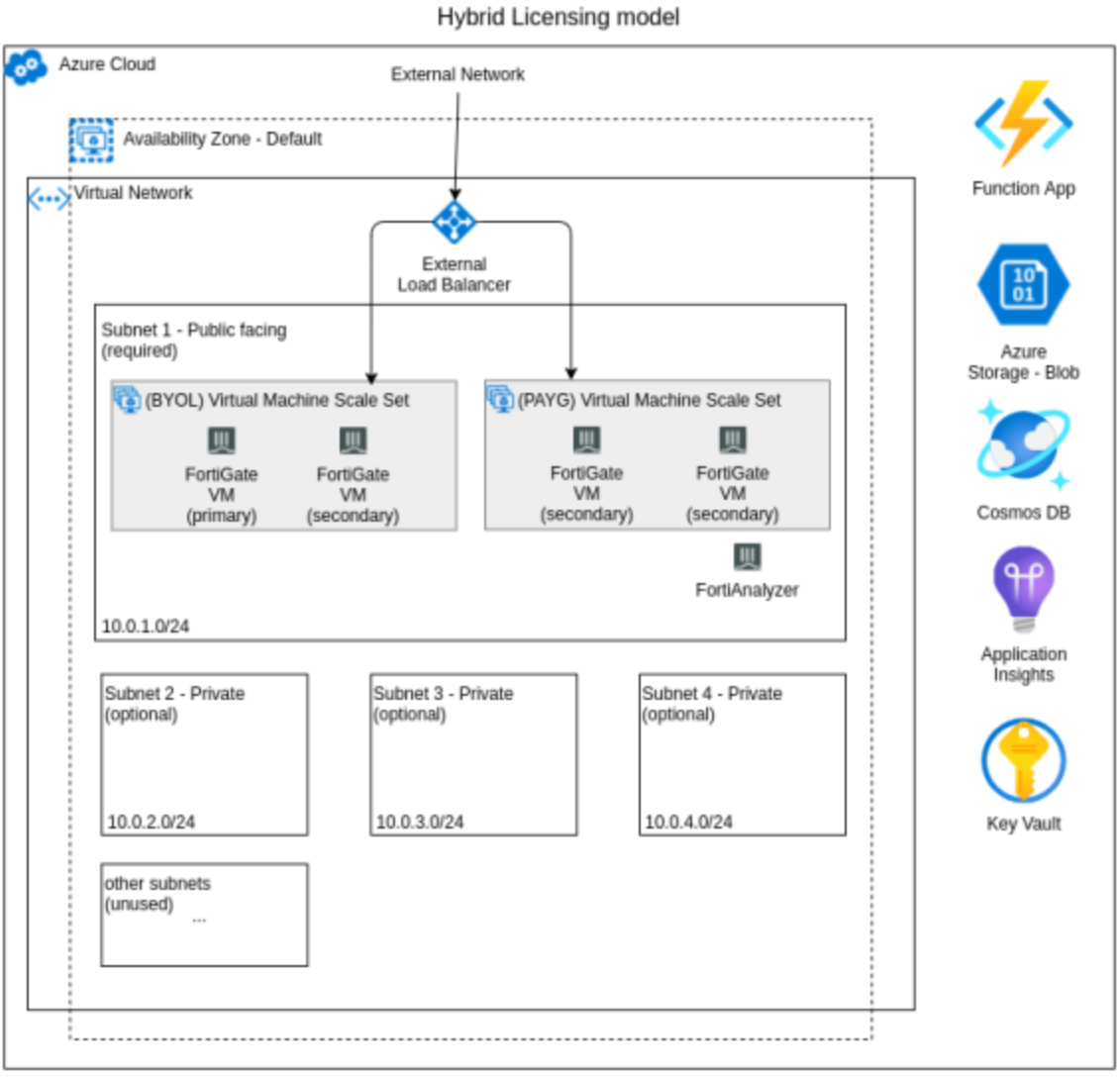
VPN output can be retrieved with this FOS CLI command:

```
# diagnose vpn tun list
```

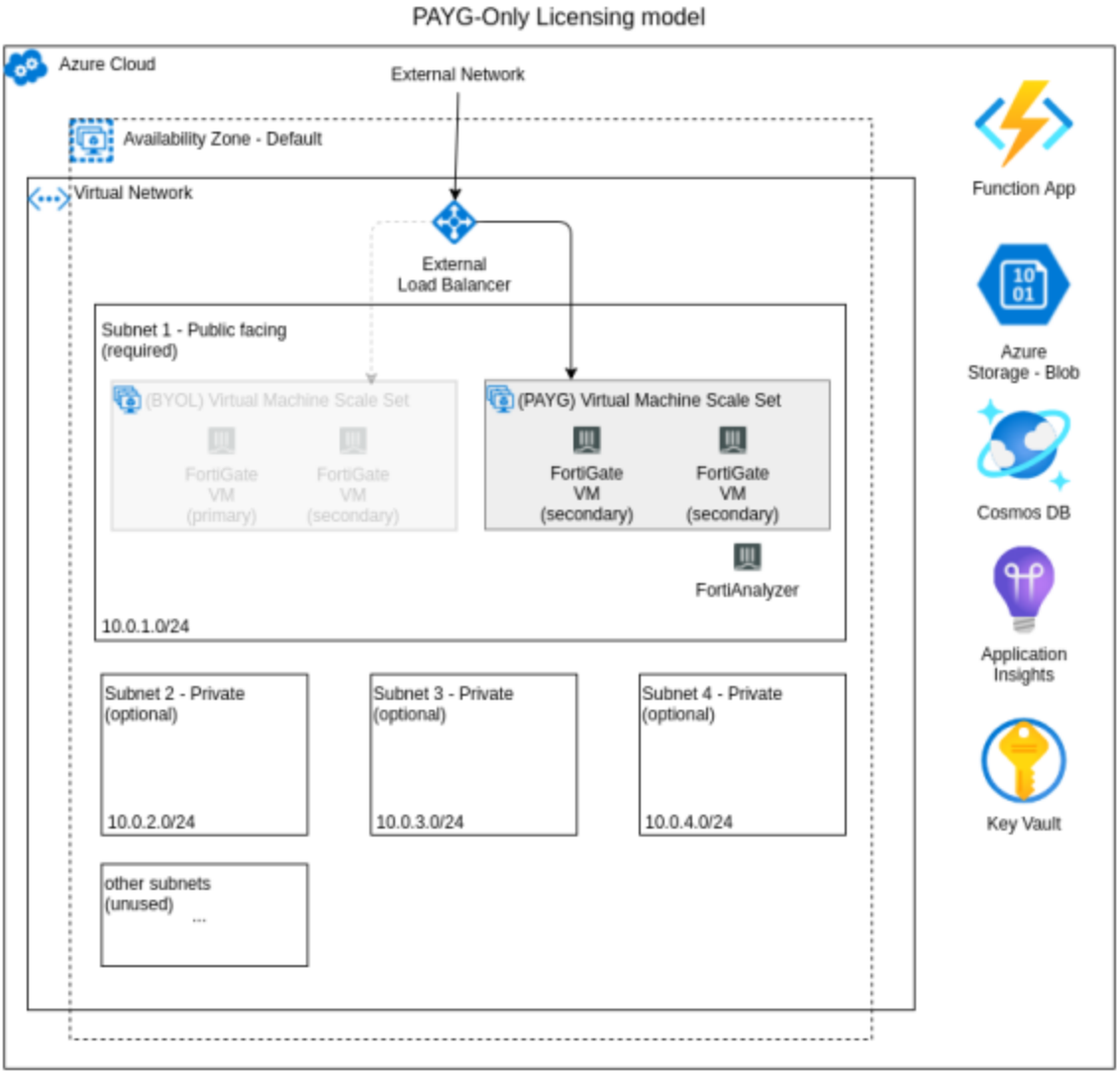
Architectural diagrams

The following diagrams illustrate the different aspects of the architecture of FortiGate Autoscale for .

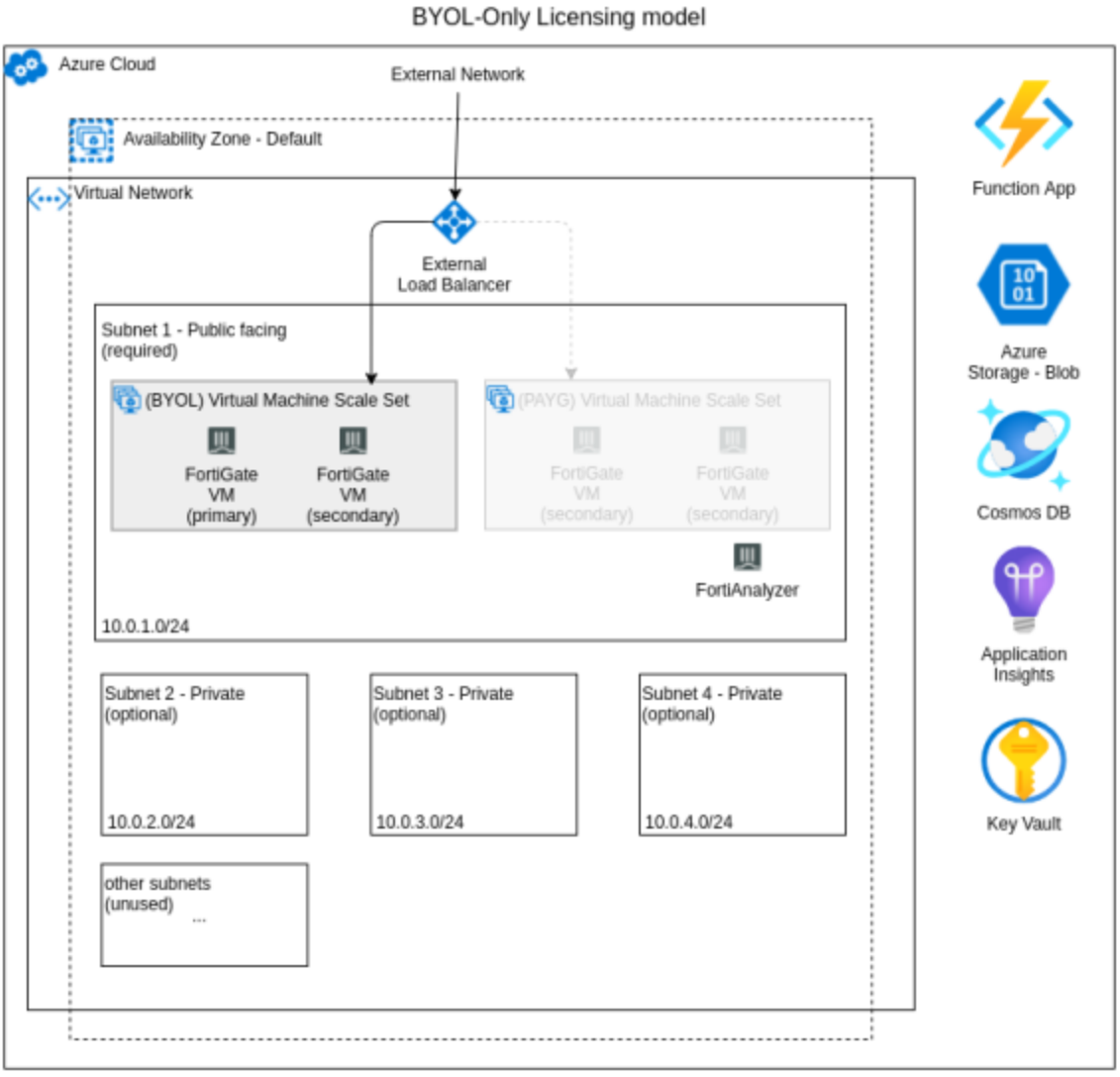
FortiGate Autoscale for Azure architecture (hybrid licensing)



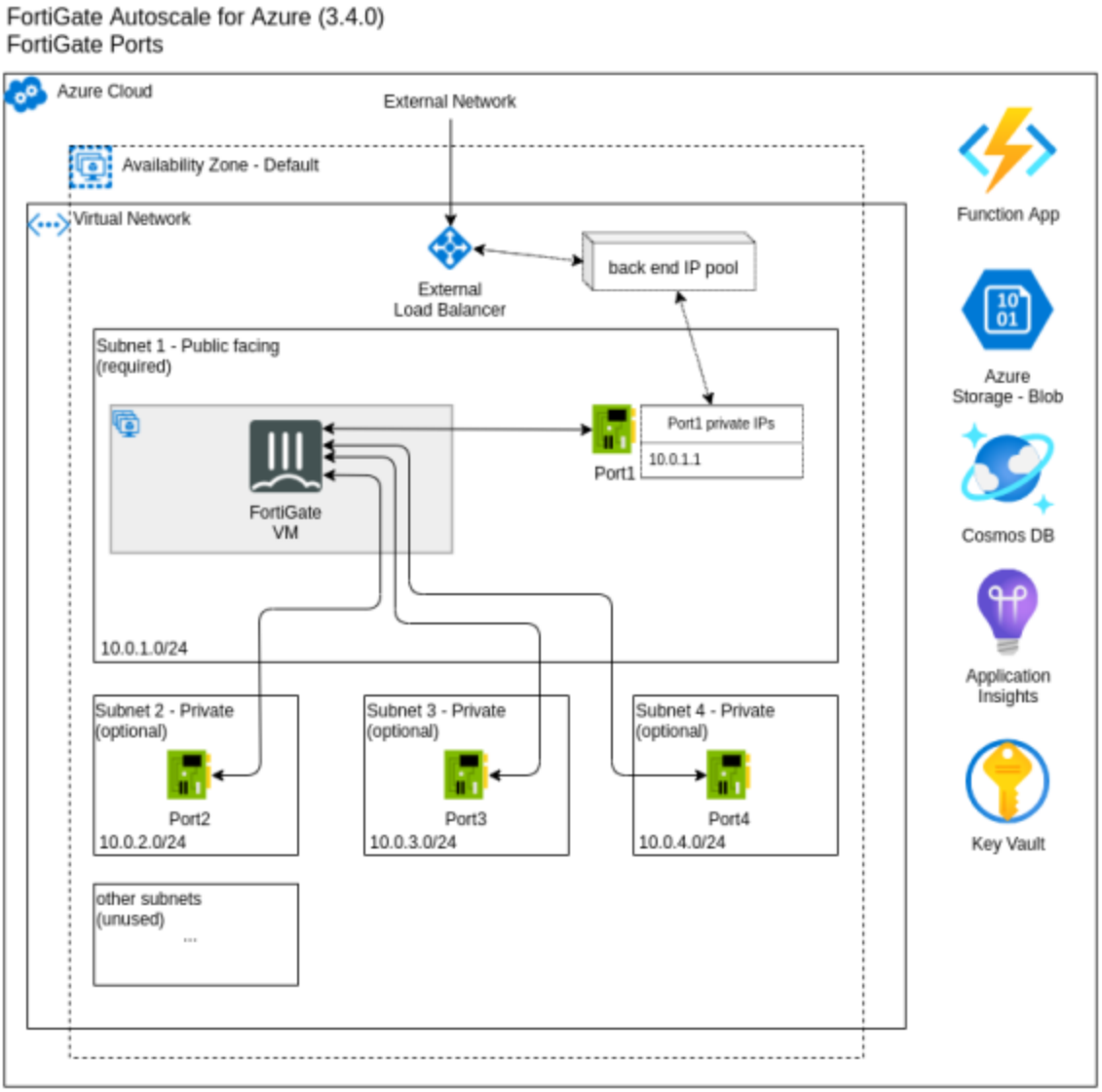
FortiGate Autoscale for Azure architecture (PAYG instances only)



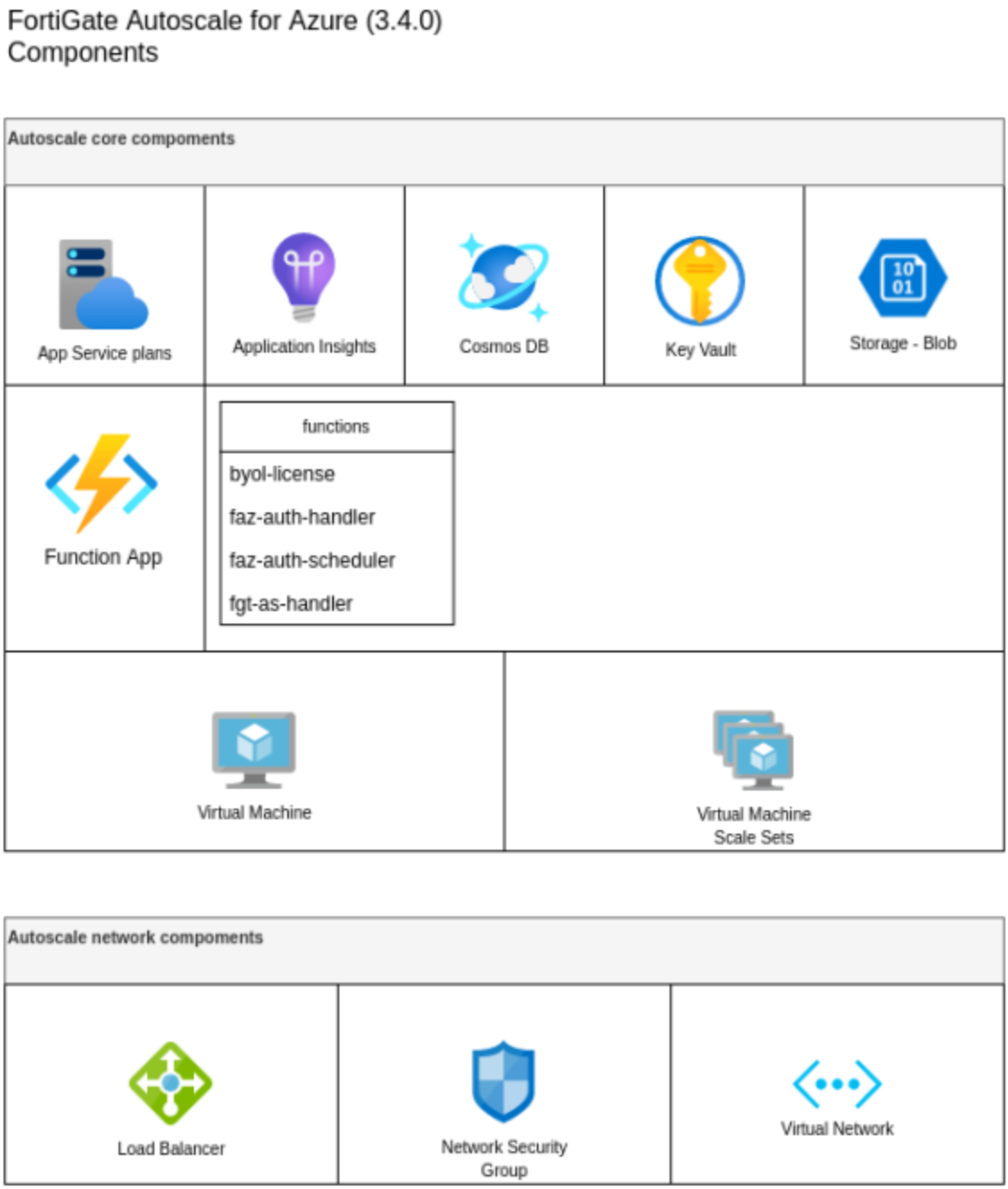
FortiGate Autoscale for Azure architecture (BYOL instances only)



FortiGate ports diagram

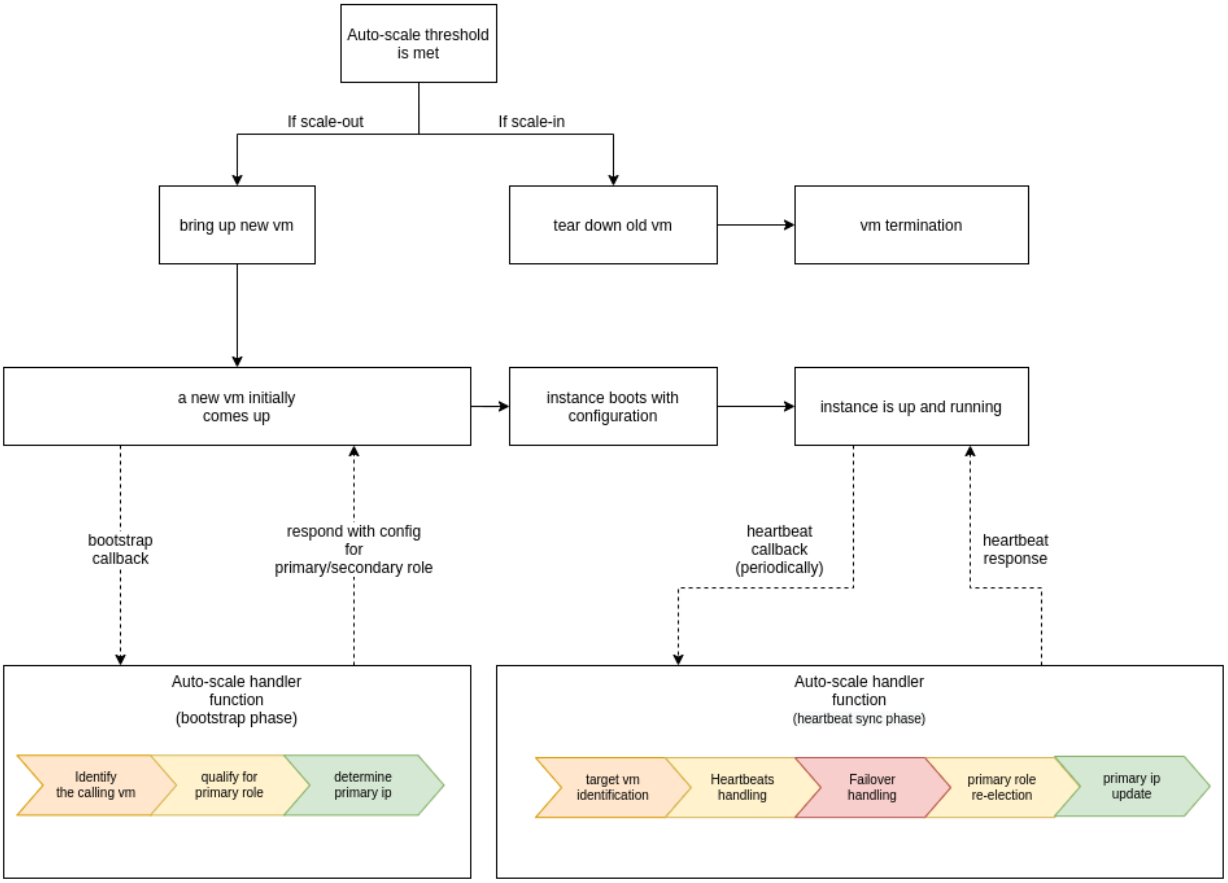


Components diagram



Autoscale handler flowchart

Autoscale handler flowchart



Upgrading the deployment

An existing FortiGate Autoscale for Azure deployment can be upgraded in one specific scenario:

- It was deployed with the 2.0.9 template.

To determine which template was used in your deployment, refer to the section Determining the FortiGate Autoscale release version on page 102.

Read these instructions completely before starting an upgrade.

A deployment with the 2.0.9 template can be upgraded only to the 3.3.2 template. During the upgrade, users can optionally consolidate logging and reporting for the FortiGate cluster by integrating FortiAnalyzer 6.2.5 or FortiAnalyzer 6.4.5.

Prerequisites for upgrading

- Linux Operating System
- NodeJS 14
- Azure CLI
- FortiGate Autoscale for Azure upgrade templates

Obtaining the upgrade templates

The FortiGate Autoscale for Azure upgrade templates are located in the Fortinet Autoscale for Azure GitHub project. Navigate to the 2.0.9 upgrade (3.3.2) release and download `fortigate-autoscale-azure.zip`.

Unzip this file on your local PC. The `templates` folder will contain these files:

- `upgrade_fortigate_autoscale_from_2.0.9_to_3.3.2.preparation.json`
  This template prepares the environment for the upgrade.
- `upgrade_fortigate_autoscale_from_2.0.9_to_3.3.2.json`
  This template performs the upgrade from the 2.0.9 template to the 3.3.2 template and pairs with the optional parameter template.
- (optional) `upgrade_fortigate_autoscale_from_2.0.9_to_3.3.2.params.json`
  This parameter template pairs with the upgrade template.
- `upgrade_fortigate_autoscale_from_2.0.9_to_3.3.2.cleanup.json`
  This template finalizes the upgrade process.

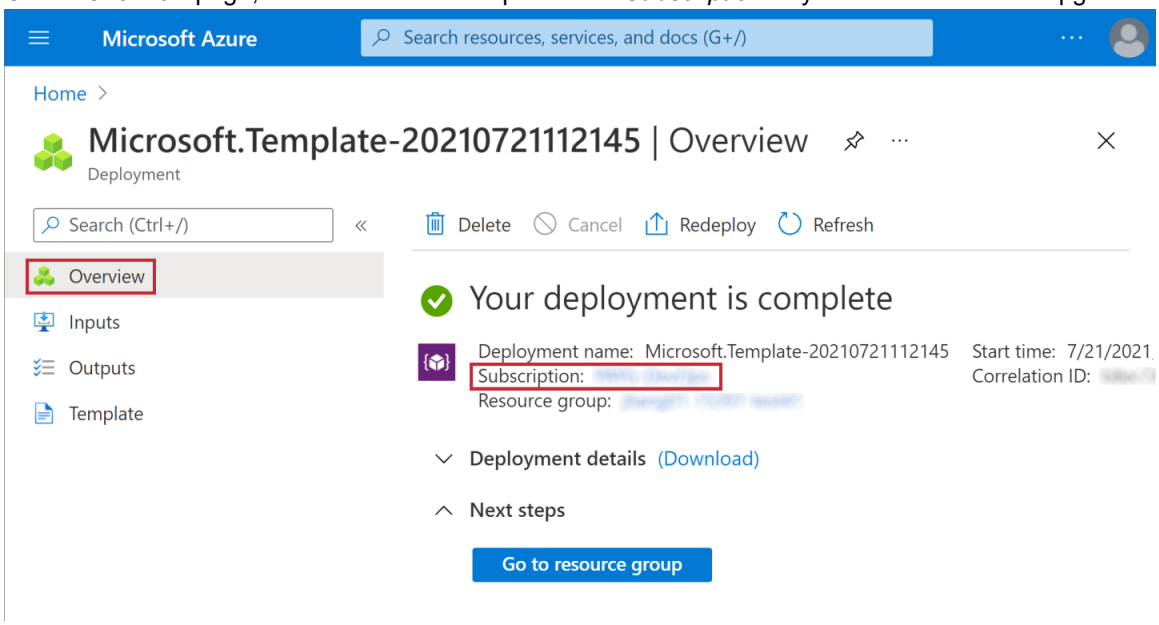
Before you start an upgrade

Upgrading the deployment requires values from the existing 2.0.9 deployment. The following sections describe how to locate these values.

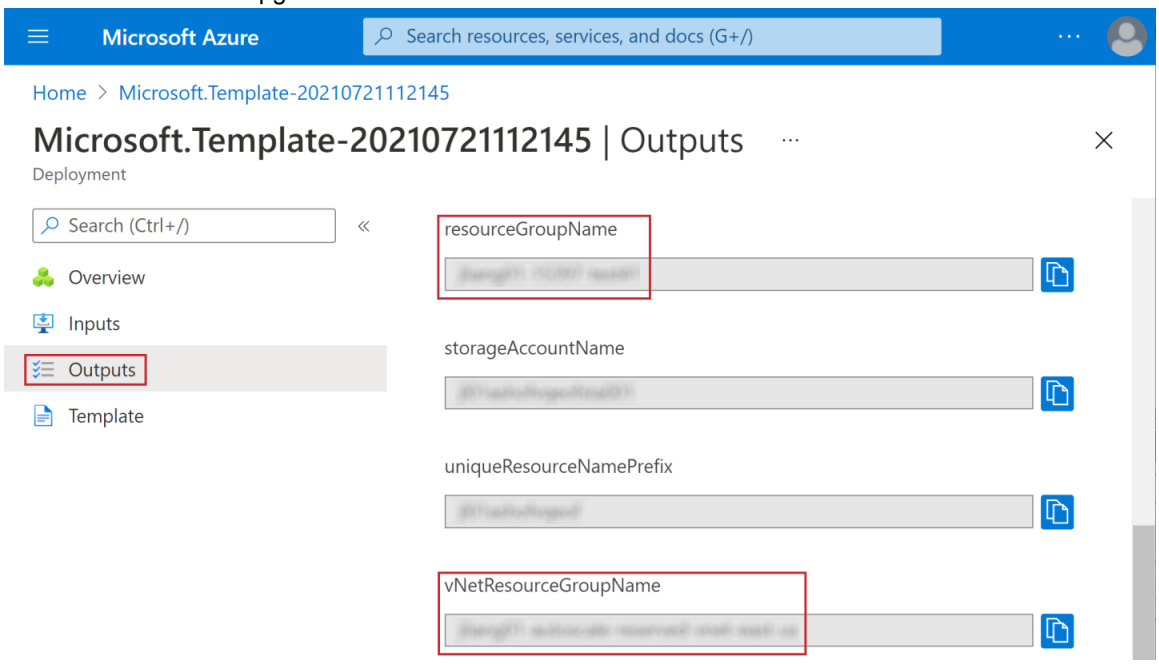
Locating values from the 2.0.9 deployment

1. Navigate to the *Microsoft.Template Overview* by following the steps 1-3 of the section Locating deployment Outputs on page 102.

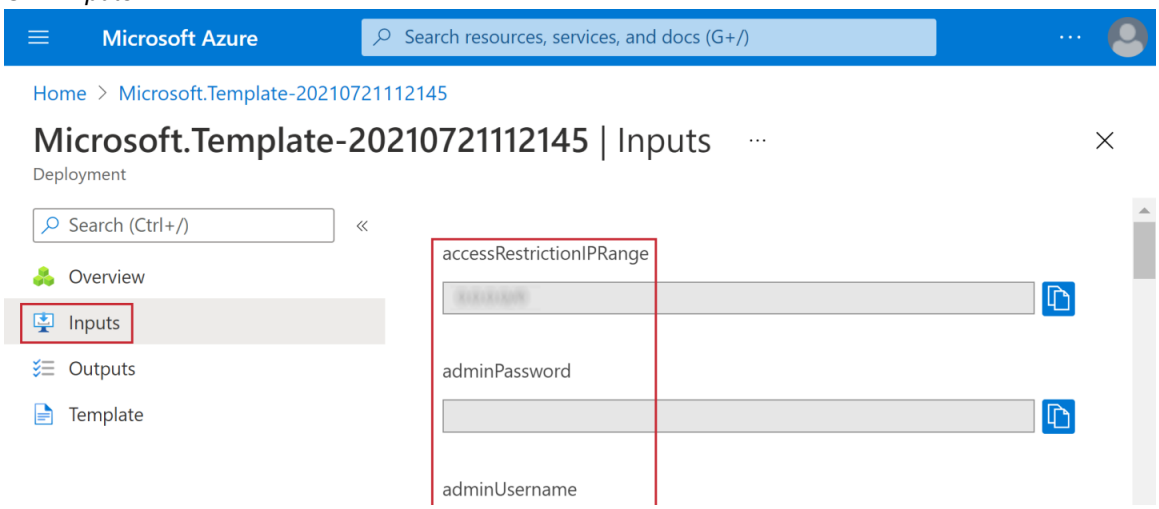
2. On the *Overview* page, note the value for the parameter *Subscription* as you will need it for the upgrade.



3. Click *Outputs*and note the values for the parameters *resourceGroupName* and *vNetResourceGroupName* as you will need them for the upgrade.



4. Click *Inputs*.



5. Make note of values on this page as you will need them for the upgrade.

Upgrade iteration

Upgrade Iteration is an important parameter throughout the entire process. The allowable values for *Upgrade Iteration* are limited to the numbers 2 thru 9. This value is used to form a unique name for the new resources related to the upgrade. If there are errors during the upgrade, the entire stack can be rolled back - the *Upgrade Iteration* value is used to remove the resources which were created.

When performing the upgrade for the first time, set *Upgrade Iteration* to 2. If errors occur, rollback the upgrade and start over with *Upgrade Iteration* set to 3. Repeat if necessary, increasing the value of *Upgrade Iteration* each time.

When a deployment is rolled back, the Key Vault will be soft-deleted. Once the Key Vault is permanently deleted, the *Upgrade Iteration* number can be reused. To permanently delete the Key Vault, open the AzureCLI and run the `upgradeIterationCmdDeleteKeyVaultPermanent` command from the *Outputs* of the cleanup template.

Performing the upgrade

The upgrade solution described here is a rollback-capable solution for preparing, creating, and removing resources. The steps below will guide you through the upgrade process.

Before starting an upgrade, ensure that the values for the 2.0.9 template deployment have been located.

1. Deploy the preparation template as described in the section Deploying the preparation template on page 126.
2. Deploy the upgrade template as described in the section Deploying the upgrade template on page 126.
3. Verify the newly deployed resources. For details, refer to the section Verifying the upgrade deployment on page 129.

Do not start the BYOL or PAYG VMSS until you initialize the database. In other words, ensure the instance number of the VMSS is set to 0.

4. Initialize the database. For details, refer to the section Initializing the database on page 129.
5. Start the two new VMSS. For details, refer to the section Starting a VMSS on page 82.
6. Observe the FortiGate-VMs running in the two VMSS and ensure they are running correctly.
7. Deploy the cleanup template. For details, refer to the section Deploying the cleanup template on page 131.

Deploying the preparation template

1. Create a template deployment using the preparation template. For details, refer to the section Creating a template deployment on page 62. When prompted for parameters, use values as described in the table below:

Parameter display name	2.0.9 template Input	2.0.9 template Ouput	Value to use
Subscription	*	*	
Resource group		resourceGroupName	Use the value from the 2.0.9 template deployment. Do not change it.
Resource Name Prefix	resourceNamePrefix		
Vnet Resource Group Name		vNetResourceGroupName	
Region	*	*	This value cannot be changed. It is tied to the Resource group.
Upgrade Iteration	*	*	Refer to the section Upgrade iteration on page 125.

* indicates that there isn't a value present in the 2.0.9 template Inputs or Outputs.

2. When deployment of the preparation template has completed, navigate to the *Outputs*. For details, refer to the section Locating deployment Outputs on page 102.
3. Copy the `cmdUpdateAllInOne` command.
4. Open a terminal in your Linux OS.
5. Log in to your Azure account with the command `az login`.
6. Run the command `cmdUpdateAllInOne`.
7. Wait for the command to be fully finished.

Deploying the upgrade template

1. Create a template deployment using the upgrade template. For details, refer to the section Creating a template deployment on page 62. For descriptions of the variables, refer to the section Configurable variables on page 66. When prompted for parameters, use values as described in the table used when creating a template deployment with the preparation template and from the table below:

Parameter display name	2.0.9 template Input	Value to use
Access Restriction IP Range	accessRestrictionIPRange	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Admin Password	adminPassword	Requires manual input. The value from the 2.0.9 template deployment is recommended; a new value may be entered.
Admin Username	adminUsername	Use the value from the 2.0.9 template deployment.
BYOL Instance Count	byolInstanceCount	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
FOS Version	fosVersion	Use values from the drop-down list. The latest version is recommended.
Forti Analyzer Autoscale Admin Password	*	Follow the instructions in the parameter description.
Forti Analyzer Autoscale Admin Username	*	
Forti Analyzer Custom Private IP Address	*	
Forti Analyzer Instance Type	*	
Forti Analyzer Integration Options	*	
Forti Analyzer Version	*	
Forti Gate PSK Secret	fortiGatePSKSecret	Requires manual input. The value from the 2.0.9 template deployment is recommended; a new value may be entered.
Heart Beat Delay Allowance	heartBeatDelayAllowance	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Heart Beat Interval	heartBeatInterval	
Heart Beat Loss Count	heartBeatLossCount	
Instance Type	instanceType	
Key Vault Name	*	Follow the instructions in the parameter description.

Parameter display name	2.0.9 template Input	Value to use
Max BYOL Instance Count	maxBYOLInstanceCount	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Max PAYG Instance Count	maxPAYGInstanceCount	
Min BYOL Instance Count	minBYOLInstanceCount	
Min PAYG Instance Count	minPAYGInstanceCount	
PAYG Instance Count	PAYGInstanceCount	
Package Res URL	packageResURL	Use the template default value. Do not change it.
Primary Election Timeout	masterElectionTimeout	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Scale In Threshold	scaleInThreshold	
Scale Out Threshold	scaleOutThreshold	
Service Plan Tier	*	Follow the instructions in the parameter description.
Service Principal App ID	restAppID	Use the value from the 2.0.9 template deployment. Do not change it
Service Principal App Secret	restAppSecret	
Service Principal Object ID	*	Follow the instructions in the parameter description.
Storage Account Type	storageAccountType	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Subnet1Name	subnet1Name	Follow the instructions in the parameter description.
Subnet2Name	subnet2Name	
Subnet3Name	subnet3Name	
Subnet4Name	subnet4Name	
Vnet Address Space	vnetAddressSpace	Use the value from the 2.0.9 template deployment. Do not change it.
Vnet Name	vnetName	

If the deployment does not complete successfully, go to the section Troubleshooting the upgrade on page 132.

2. Upload `configset` files to the Storage account. For details, refer to the section Uploading files to the Storage account on page 72.
3. If you will be using BYOL instances, upload `license` files to the Storage account.

License files from the 2.0.9 deployment can be reused . However, re-using a license will invalidate the FortiGate which is currently using the license.

Verifying the upgrade deployment

The FortiGate Autoscale for Azure 3.3.2 template will be deployed into the Resource Group and a new set of the following 6 resources will be created:

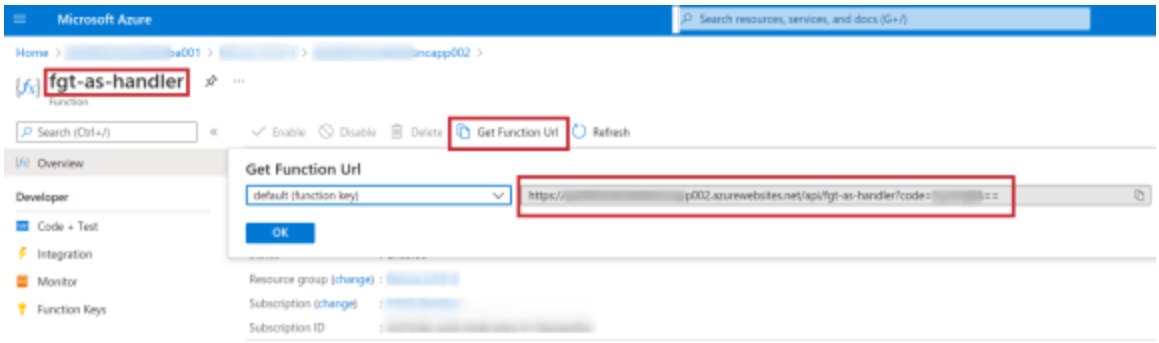
- Function App
- App Service plan
- Application Insights
- Storage account
- Azure Cosmos DB account
- Virtual machine scale set (BYOL)
- Virtual machine scale set (PAYG)

These resources will be created with the same name as the previous 2.0.9 resources with the iteration number appended. For example, if the Upgrade Iteration is 2, the number appended is 002. Verify that they have been created. For details on verifying components, refer to the section Verifying the deployment on page 74.

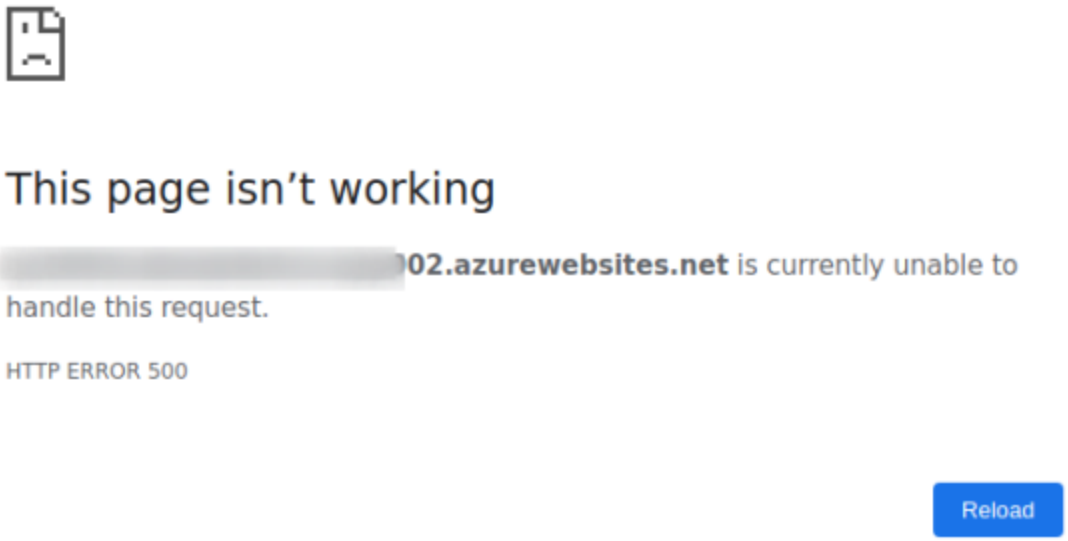
Initializing the database

Do not scale out the BYOL or PAYG VMSS until you initialize the database.

1. Navigate to the `fgt-as-handler` function. For details on how to do this, refer to the section To verify the Function App: on page 76.
2. Click *Get Function Url* to obtain the Function URL:

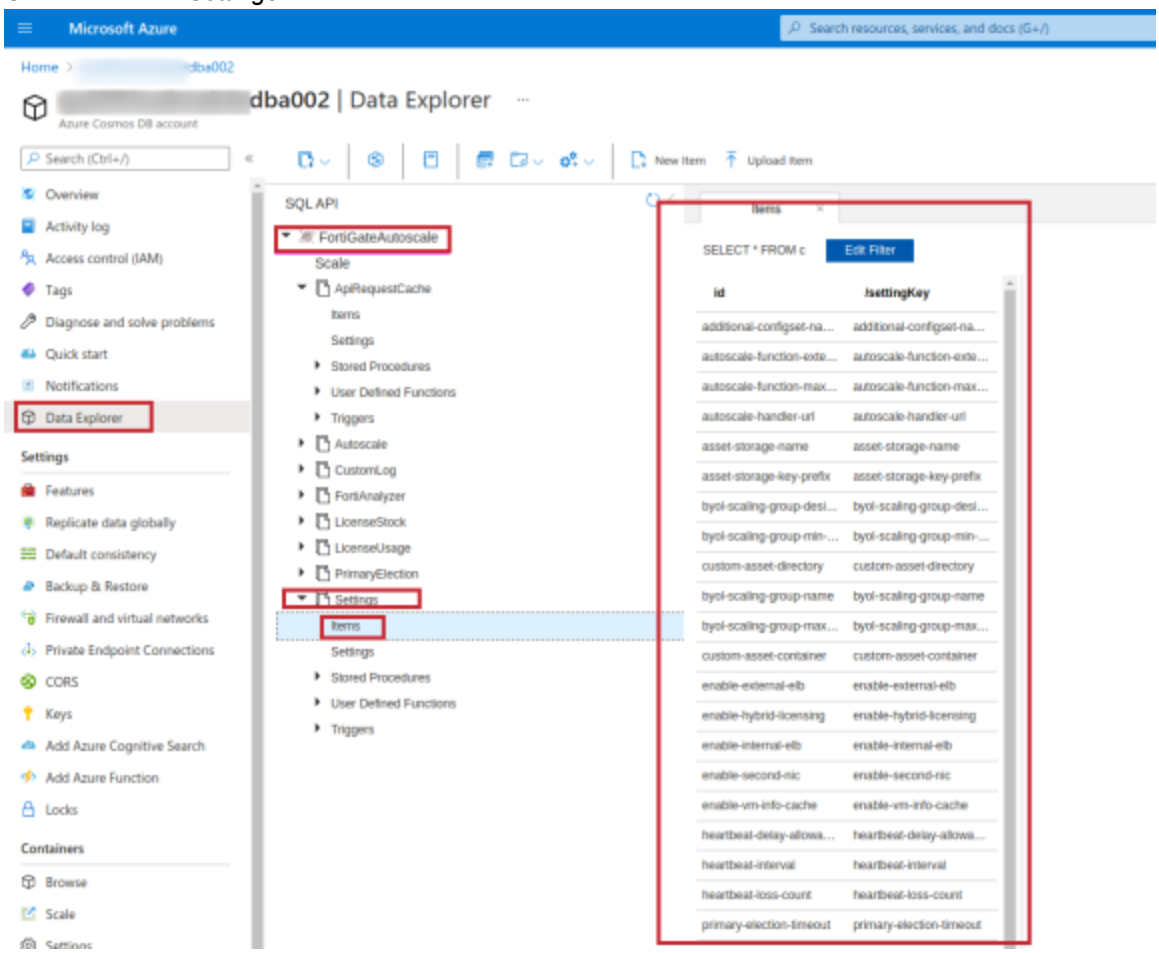


3. Open a web browser to run the URL. The expected response is an error as shown below:



4. Navigate to the cosmos DB account of the current upgrade iteration. For details on how to do this, refer to steps 1 and 2 in the section To verify the database: on page 76.
5. On the right hand side, expand the database *FortiGateAutoscale*.
6. Expand the container *Settings*.
7. Click on *Items*.

8. Confirm that the *Settings* container has items.



Deploying the cleanup template

1. Create a template deployment using the cleanup template. For details, refer to the section Creating a template deployment on page 62. When prompted for parameters, use values as described in the table below:

Parameter display name	2.0.9 template Input	2.0.9 template Ouput	Value to use
Subscription	*	*	
Resource group		resourceGroupName	Use the value from the 2.0.9 template deployment. Do not change it.
Resource Name Prefix	resourceNamePrefix		
Vnet Resource Group Name		vNetResourceGroupName	
Region	*	*	This value cannot be changed. It is tied to the Resource group.

Parameter display name	2.0.9 template Input	2.0.9 template Ouput	Value to use
Upgrade Iteration	*	*	Use the iteration number for the upgrade iteration you want to continue with

* indicates that there isn't a value present in the 2.0.9 template Inputs or Outputs.

2. When deployment of the cleanup template has completed, navigate to the *Outputs*.
3. Copy the command appropriate for your activity:
   - To finalize the upgrade, copy the `cleanUpOldComponentCmdDeleteAllInOne` command.
   - To roll back the upgrade, copy the `upgradeIterationCmdDeleteAllInOne` command.
4. Open a terminal in your Linux OS.
5. Log in to your Azure account with the command `az login`.
6. Run the copied command.
7. Wait for the command to be fully finished.

Troubleshooting the upgrade

As long as an upgrade process isn't finalized, it is regarded as an incomplete upgrade iteration. Reasons for not finalizing can include errors and user intervention.

In the case of an incomplete upgrade iteration, roll back the upgrade iterationand perform the upgrade again with a different value for *Upgrade Iteration*. It is suggested that the value be increased by 1 with each successive deployment.

Rolling back an incomplete upgrade iteration

Users have the option of rolling back an upgrade iteration by deploying the cleanup template. When deployed, newly created resources related to the upgrade iteration will be released. It is recommended to rollback right away before starting a new upgrade iteration. This option must be used if all the allowable *Upgradte Iteration* values (2-9) have been used up.

When a deployment is rolled back, the Key Vault will be soft-deleted. Once the Key Vault is permanently deleted, the *Upgrade Iteration* number can be reused. To permanently delete the Key Vault, open the AzureCLI and run the `upgradeIterationCmdDeleteKeyVaultPermanent` command from the *Outputs* of the cleanup template.

Document history

Template	Date Released	Details
3.4.0	November 22, 2021	Added support for deployment of 1 - 4 subnets. (Previously 4 were deployed). Added support for failover recovery. (Updated Failover management parameters).

Template	Date Released	Details
special release	August 25, 2021	This special release is for upgrading from the 2.0.9 template to the 3.3.2 template. The upgrade release package is located on the Fortinet Autoscale for Azure release page tag 2.0.9 upgrade (3.3.2).
3.3.2	June 11, 2021	Documentation was not updated.
3.3.0	May 25, 2021	Added support for FortiAnalyzer.
3.1.1	February 4, 2021	Added support for FortiOS 6.4.3. Removed support for FortiOS 6.2.x.
3.0.0	September 23, 2020	Added support for FortiOS 6.2.3.
2.0.5	February 25, 2020	Added support for FortiOS 6.0.9.
2.0	October 8, 2019	FortiGate Autoscale 2.0.0 General Availability Added support for Hybrid Licensing (any combination of BYOL and/or PAYG instances).
1.0	April 19, 2019	FortiGate Autoscale General Availability Supports auto scaling for PAYG instances only. Requires FortiOS 6.0.6 or FortiOS 6.2.1. Documentation is no longer maintained and is only available as a PDF: • Deploying auto scaling on Azure 1.0

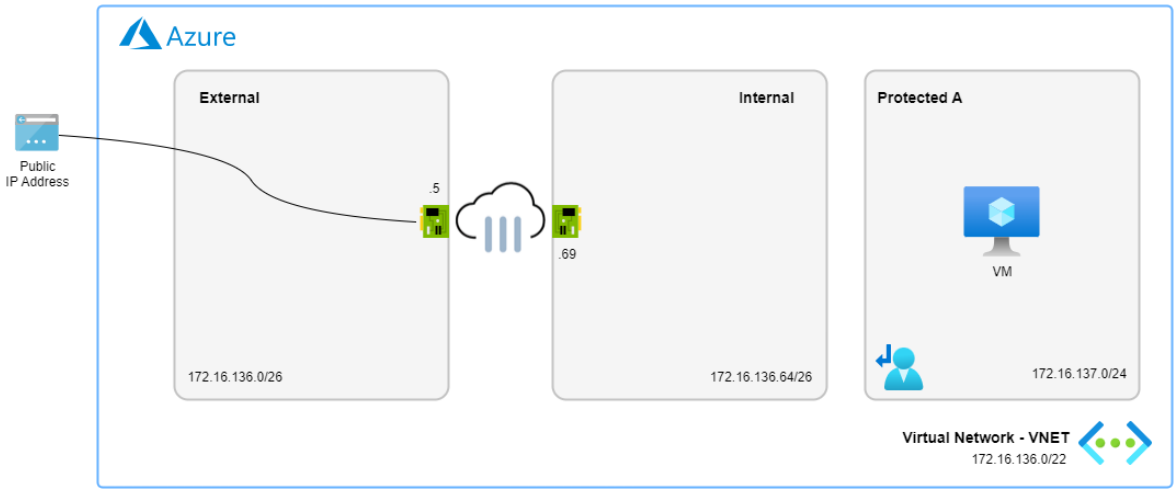
Single FortiGate-VM deployment

You can deploy FortiGate-VM next generation firewall (NGFW) for Azure as a virtual appliance in the Azure cloud (infrastructure as a service (IaaS)). This section shows you how to install and configure a single instance FortiGate-VM in Azure to provide a full NGFW/unified threat management security solution in front of Azure IaaS resources.

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 multitiered solutions.

The example in this document creates three subnets:

Subnet	Description
Subnet1	External subnet used to connect the FortiGate-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 FortiGate for inspection using UDR.



Registering and downloading your license

FortiGate-VM for Azure supports bring your own license (BYOL) and pay as you go licensing models. If you are deploying a FortiGate-VM in the Azure marketplace with BYOL, you must obtain a license to activate it.

You can obtain licenses through any Fortinet partner. If you do not have a partner, contact azuresales@fortinet.com for assistance in purchasing a license.

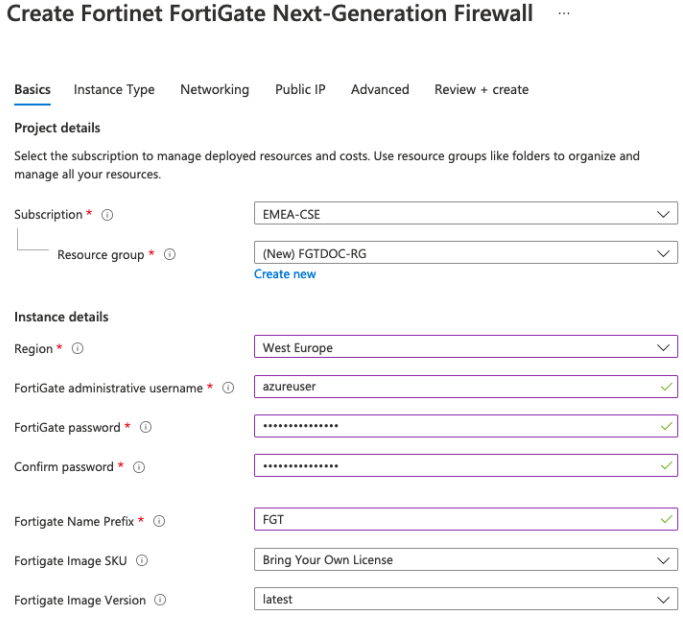
See Creating a support account on page 16.

Deploying the FortiGate-VM

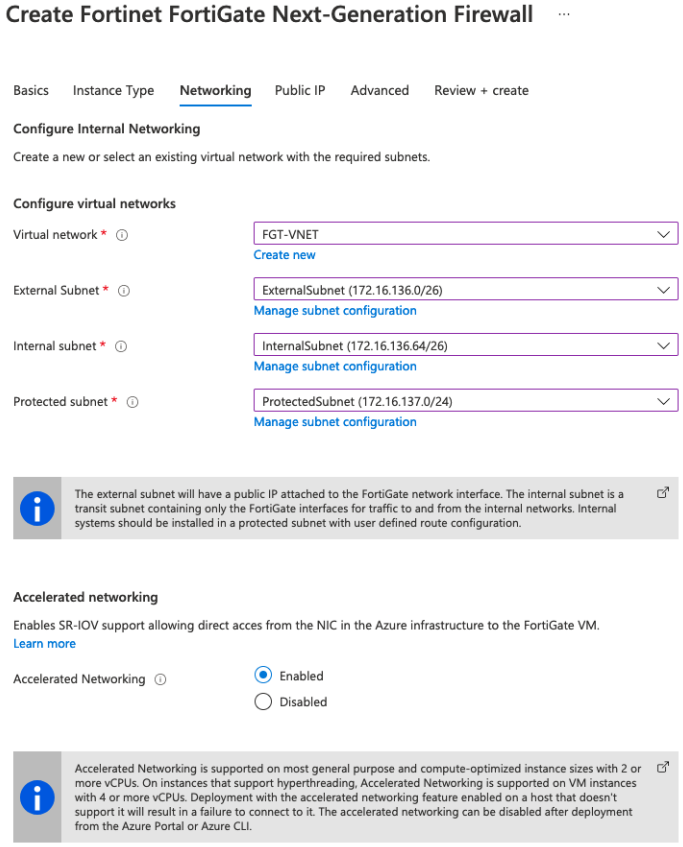
There are different deployment methods for the FortiGate-VM related to the different deployment methods that the Azure platform supports. This guide focuses on the Azure portal. This offers a convenient and guided deployment. For more automated deployment, ARM templates or Terraform are available on the Fortinet GitHub. See Deploying FortiGate with a custom ARM template on page 24.

To deploy the FortiGate-VM:

1. In the Azure dashboard, select *Create a resource* and search for FortiGate.
2. Locate the Fortinet FortiGate Next-Generation Firewall listing and select it.
3. From the *Select a plan* dropdown list, select *Single VM*. Click *Create*.
4. 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. FortiGate-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 *FortiGate administrative username* field, enter the username that you will use to manage the FortiGate. The username cannot be a common username such as root, admin, or administrator. After deployment, you can reset the username and password from the Azure portal interface, resulting in a system reboot.
   d. In the *FortiGate password* field, enter the password used to manage the FortiGate via the GUI or CLI. The password must be at least twelve characters and contain one or more of the following tokens: uppercase letters, lowercase letters, digits, and special characters: ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/.
   e. In the *Fortigate Name Prefix* field, enter the desired prefix. All resources contain the prefix in their name.
   f. From the *Fortigate Image SKU* dropdown list, select the license type. Pay as you go is billed through Azure as an additional charge to compute usage.
   g. From the *Fortigate Image Version* dropdown list, select the desired FortiGate version. The default option installs the latest FortiGate version.



5. For *Instance Type*, select the instance type according to the purchased bring your own license (BYOL) license or the anticipated cost per hour. Licensing is based on the number of utilized vCPUs. You can resize the VM later if needed. See Instance type support on page 6.
6. On the *Networking* tab, configure the following:
   a. Configure the networks. You can deploy the FortiGate in an existing VNet or create a new VNet. If deploying to an existing VNet, you must already have three subnets to use for the FortiGate-VM. The FortiGate-VM requires a public and private interface for Internet edge protection. Ensuring that the external and internal subnets of the FortiGate are empty or do not contain other networking devices that require routing is recommended.
   b. Enable *Accelerated Networking* if desired. You can enable this option to have a direct path from the VM to the Azure infrastructure NIC and allows for better performance. This is only available for specific instance types. See Enabling accelerated networking on the FortiGate-VM on page 43.



7. On the *Public IP* tab, create a new public IP address or select an existing unattached public IP address. The public IP address can be a basic or standard SKU public IP address. A highly available setup requires a standard SKU public IP address. Upgrading from a basic to a standard SKU public IP address is supported. See Upgrade public IP addresses.
8. On the *Advanced* tab, configure the following:
   a. In the *FortiManager* section, provide FortiManager details if desired. During deployment, the FortiGate can reach out and register itself to a FortiManager using the provided details.
   b. In the *Custom Data* field, add additional configuration if desired. This provides a configuration to the FortiGate during deployment. For example, you can enter FortiOS CLI commands.
   c. If using a BYOL license, upload the license so that it can be provided during deployment to the FortiGate.

9. Launch the FortiGate deployment:
   a. You are finished configuring the options. Once validation passes, click *OK*.

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

   b. Click *Create*. After deploying the template, you should see the deployment progress and the parameters and template that Azure is progressing. Once deployed, the new resources show in the resource group.

Connecting to the FortiGate-VM

To connect to the FortiGate-VM:

1. Open the FGTPublicIP resource and copy the IP address that Azure assigned.
2. In a web browser, connect to the IP address using HTTPS on port 443. You can also use an SSH client on port 22.
3. The system displays a warning that the certificate is untrusted. This is expected since the FortiGate-VM is using a self-signed certificate. If desired, replace the certificate with a signed certificate.
4. Sign in with the credentials specified in the Azure template parameters.
5. If you chose a bring your own license deployment, you must upload a license and reboot the FortiGate-VM before continuing. See Registering and downloading your license on page 134.

Azure routing and network interfaces

On the Azure platform and the FortiGate-VM, the private IP addresses of both interfaces are configured using static assignment using deployment.

In the static routing, a default route has been configured towards the default gateway of the external network on port1. All internal networks are routed to the internal/transit network on port2. The gateway IP address on the Microsoft side is always the first IP address in the subnet IP address range.

Azure uses the 168.63.129.16 address for various services. You can configure an additional route to ensure that this traffic always leaves via port1. See What is IP address 168.63.129.16?

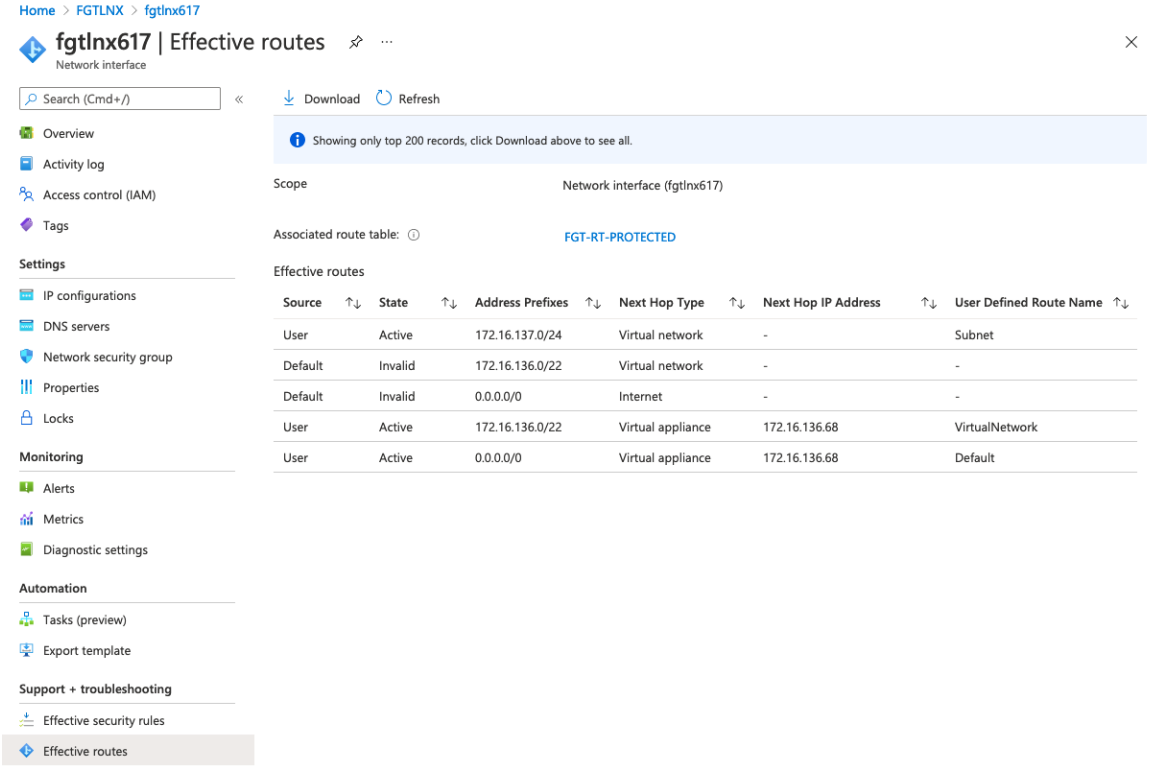
During deployment, a route table is created and attached to the protected subnet. This routing table contains three user-defined routes. The default route 0.0.0.0/0 points to the FortiGate-VM internal IP address. This catches all traffic except for the virtual network traffic and sends it to the FortiGate-VM for inspection.

The virtual network is created as well and forces traffic for additional protected networks to pass through the FortiGate-VM. As Azure applies these subnet routes to each VM, an additional route is needed for the local subnet to send its traffic directly to the VNet. If this route is omitted, you will have microsegmentation sending all traffic between the VMs in the protected subnet also via the FortiGate-VM.

If no internal segmentation is required, you can delete the VNet routes.

Verify that the route table is attached to the ProtectedSubnet. Ensure that the UDR routes include the destination networks.

To verify and troubleshoot routing, you can request the effective route tables from each network interface of a running VM. The screenshot shows that the UDR deployed within the FortiGate invalidated the default routes.

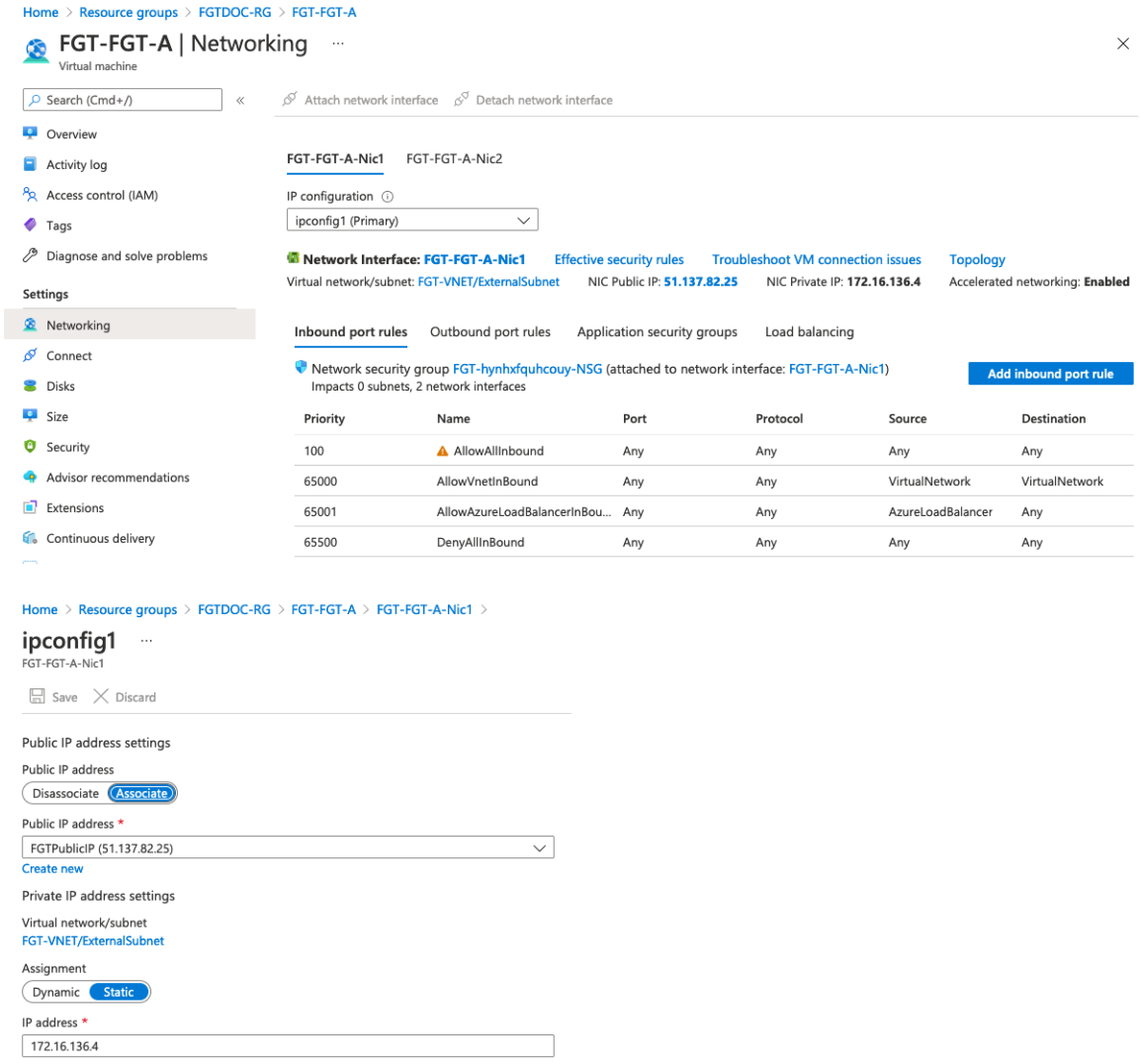


Using public IP addresses

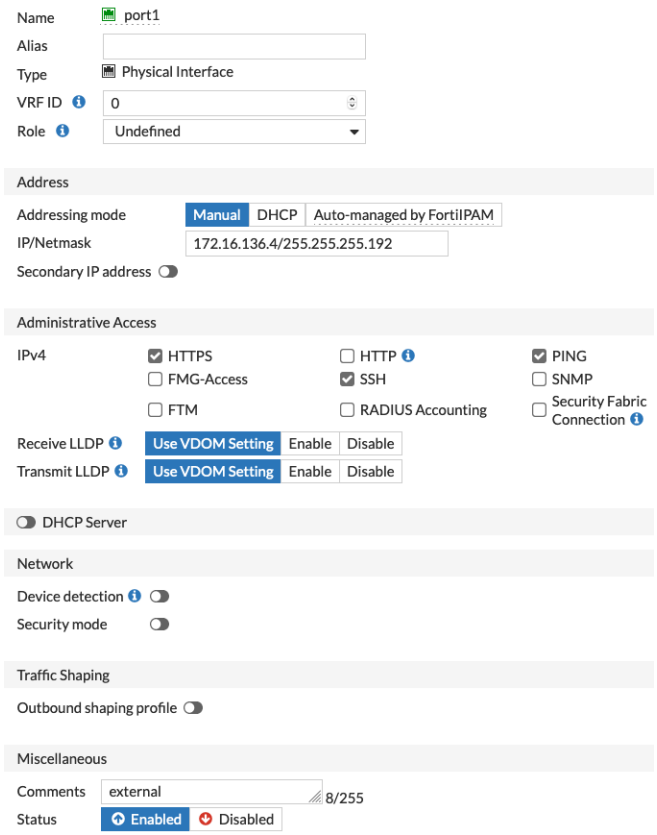
Azure does not publicly route IP addresses within a VNet, so you cannot assign a public IP address to another VM and still filter that traffic through a FortiGate-VM on Azure. Instead, you must assign the public IP addresses to the vNICs associated with the FortiGate-VM, then configure the FortiGate-VM to forward that traffic. Further, in most cases, Azure provides 1:1 NAT between the assigned public IP address and the assigned local IP address. Thus, the FortiGate-VM must forward packets using the local IP address.

A single FortiGate-VM deployment from the Azure marketplace includes one Azure IP address configuration containing a public IP address and a local IP address. Azure performs 1:1 NAT between the two as traffic enters and exits the VNet. This configuration is called an instance-level public IP address. All types of protocols are forwarded using NAT from an external public IP address to the FortiGate private IP address that is linked to it in the network interface on Azure.

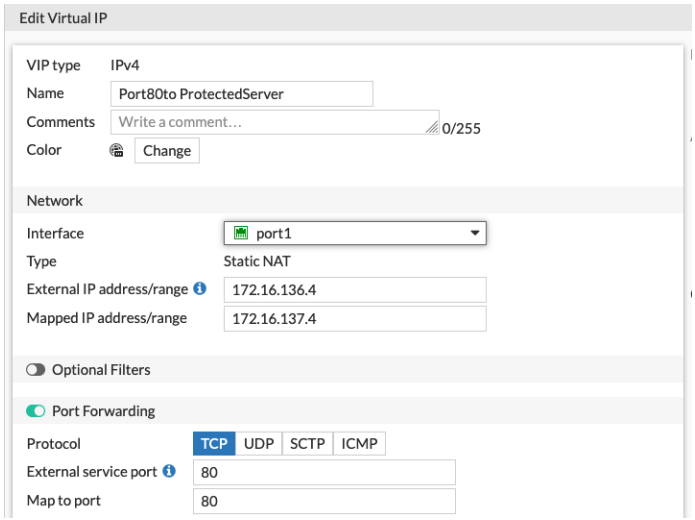
The following shows the default Azure vNIC and FortiOS configurations:


Home > Resource groups > FGTDOC-RG > FGT-FGT-A
FGT-FGT-A | Networking
Virtual machine
Search (Cmd+/)
Attach network interface
Detach network interface
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Security
Advisor recommendations
Extensions
Continuous delivery
FGT-FGT-A-Nic1
FGT-FGT-A-Nic2
IP configuration
ipconfig1 (Primary)
Network Interface: FGT-FGT-A-Nic1
Effective security rules
Troubleshoot VM connection issues
Topology
Virtual network/subnet: FGT-VNET/ExternalSubnet
NIC Public IP: 51.137.82.25
NIC Private IP: 172.16.136.4
Accelerated networking: Enabled
Inbound port rules
Outbound port rules
Application security groups
Load balancing
Network security group FGT-hynhxfquhcouy-NSG (attached to network interface: FGT-FGT-A-Nic1)
Impacts 0 subnets, 2 network interfaces
Add inbound port rule
Priority
Name
Port
Protocol
Source
Destination
100
AllowAllInbound
Any
Any
Any
Any
65000
AllowVnetInBound
Any
Any
VirtualNetwork
VirtualNetwork
65001
AllowAzureLoadBalancerInBou...
Any
Any
AzureLoadBalancer
Any
65500
DenyAllInBound
Any
Any
Any
Any

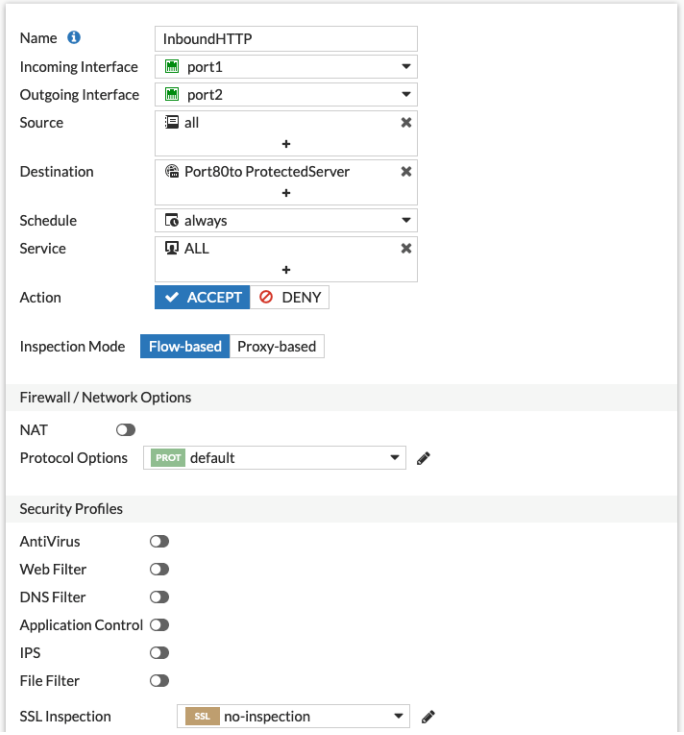
Home > Resource groups > FGTDOC-RG > FGT-FGT-A > FGT-FGT-A-Nic1 >
ipconfig1
FGT-FGT-A-Nic1
Save
Discard
Public IP address settings
Public IP address
Disassociate
Associate
Public IP address *
FGTPublicIP (51.137.82.25)
Create new
Private IP address settings
Virtual network/subnet
FGT-VNET/ExternalSubnet
Assignment
Dynamic
Static
IP address *
172.16.136.4



To use this public IP address for public access to an internal server, you must configure a virtual IP address, which enables a DNAT conversion of packets, and a policy to allow the traffic.

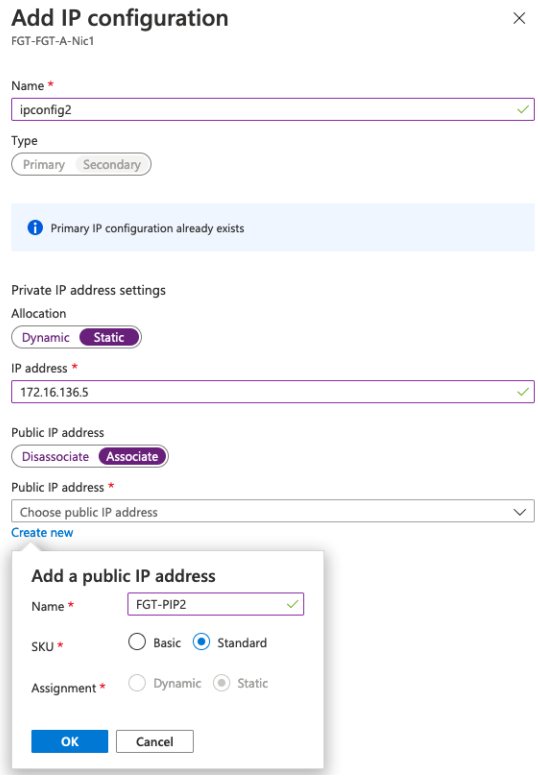


The external IP address matches the local IP address assigned to port1. The mapped IP address in this case is the internal web server's IP address, and only TCP port 80 is set to forward. You can also use PAT here to modify the original destination port in cases where there is a mismatch with the internal server's destination port. Using this feature, you can configure multiple virtual IP addresses to internal web servers using TCP port 80 by using custom external ports (8080 in this example). However, for each assigned local IP address, you can only use any given external TCP port once.



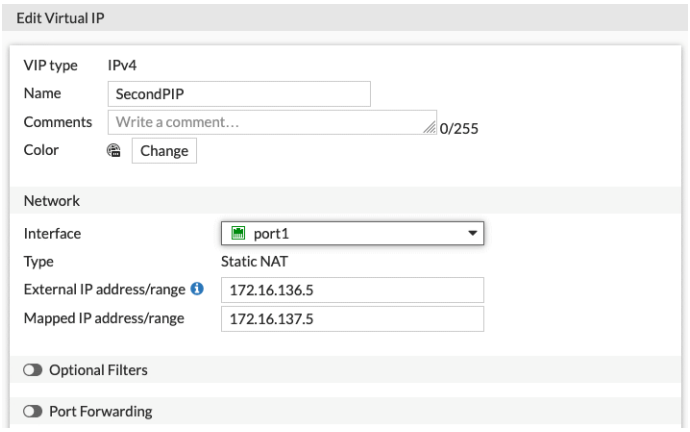
Here the policy is set to allow traffic coming in port1 to exit port2 if it is destined to the previously created virtual IP address.

To add a public IP address, create a new IP address configuration for the vNIC in the Azure portal. Click the *Add* button in *IP configurations* in the vNIC resource view.

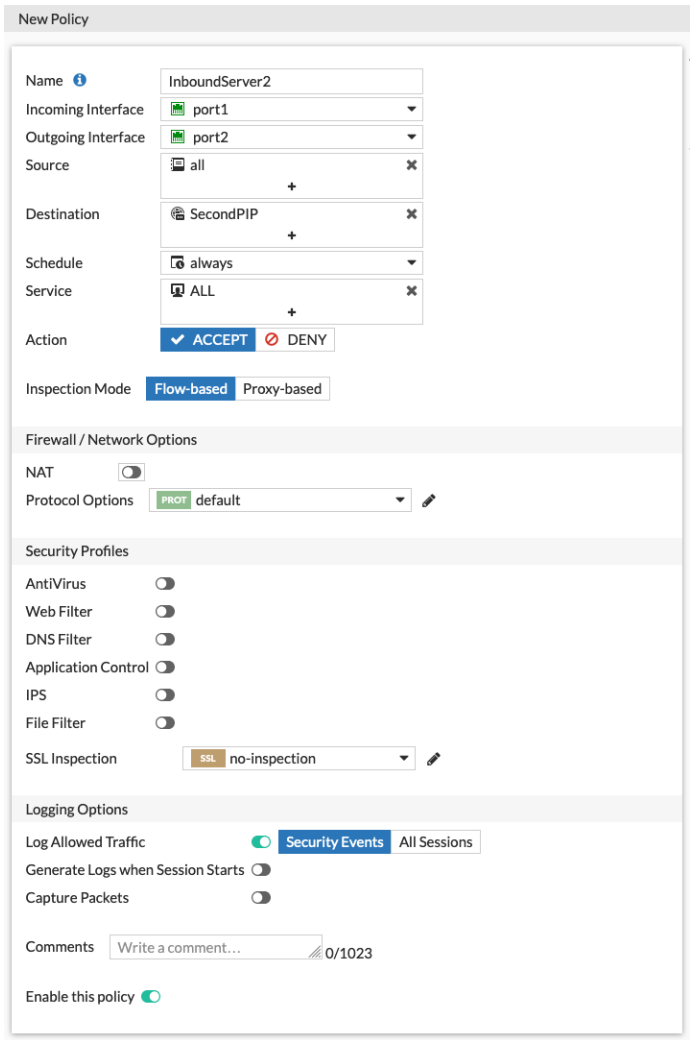


The new local address should be static and must be in the same subnet as the primary IP address configuration. Enable the public IP address and create a new public IP address resource or select an existing one. If you have an existing public IP address assigned to an internal server, you can first dissociate it from that vNIC, then assign it here.

Once you have configured both IP addresses on the Azure side, you can create an additional virtual IP address on the FortiGate-VM. You do not need to modify the interface configuration on the FortiGate-VM.



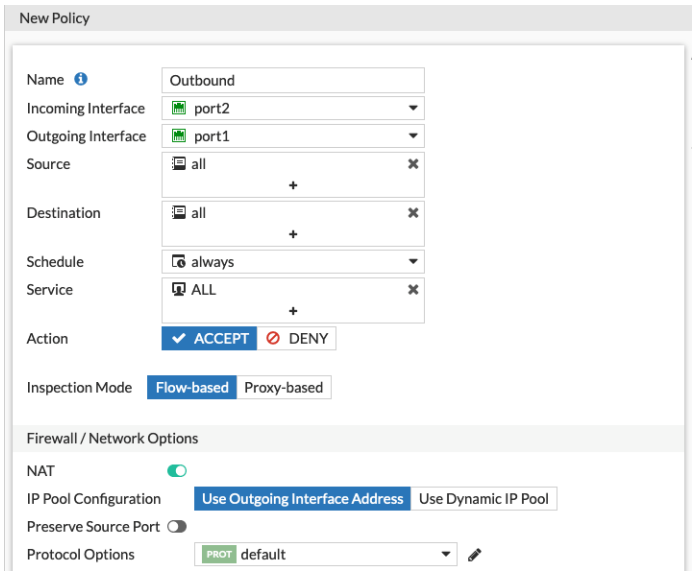
In this example, port forwarding is disabled. You can enable port forwarding if you want to forward only a specific TCP or UDP port or port range. If you do not enable port forwarding, this enables forwarding of all ports designated to the new public IP address to the internal server, in this case at 172.16.137.5



This policy matches the new virtual IP address destination and also allows all services to be forwarded. You can repeat this process for adding as many public IP addresses as needed, although you may run into Azure quota limitations.

When configuring an outbound rule for your server, you can create a general rule. All traffic is NATed behind the external interface private IP address. Azure SNATs these packets subsequently to the linked instance-level public IP address.

Outgoing traffic for the secondary server behind the secondary VIP, without the port configuration, automatically SNATs behind the external IP address in the VIP.


New Policy
Name
Outbound
Incoming Interface
port2
Outgoing Interface
port1
Source
all
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT
IP Pool Configuration
Use Outgoing Interface Address
Use Dynamic IP Pool
Preserve Source Port
Protocol Options
PROT
default

HA for FortiGate-VM on Azure

You can use FortiGate-VM in different scenarios to protect assets that are deployed in Azure virtual networks (VNet):

- Secure hybrid cloud
- Cloud security services hub
- Logical intent-based segmentation
- Secure remote access

See Cloud Security for Azure for a general overview of different public cloud use cases.

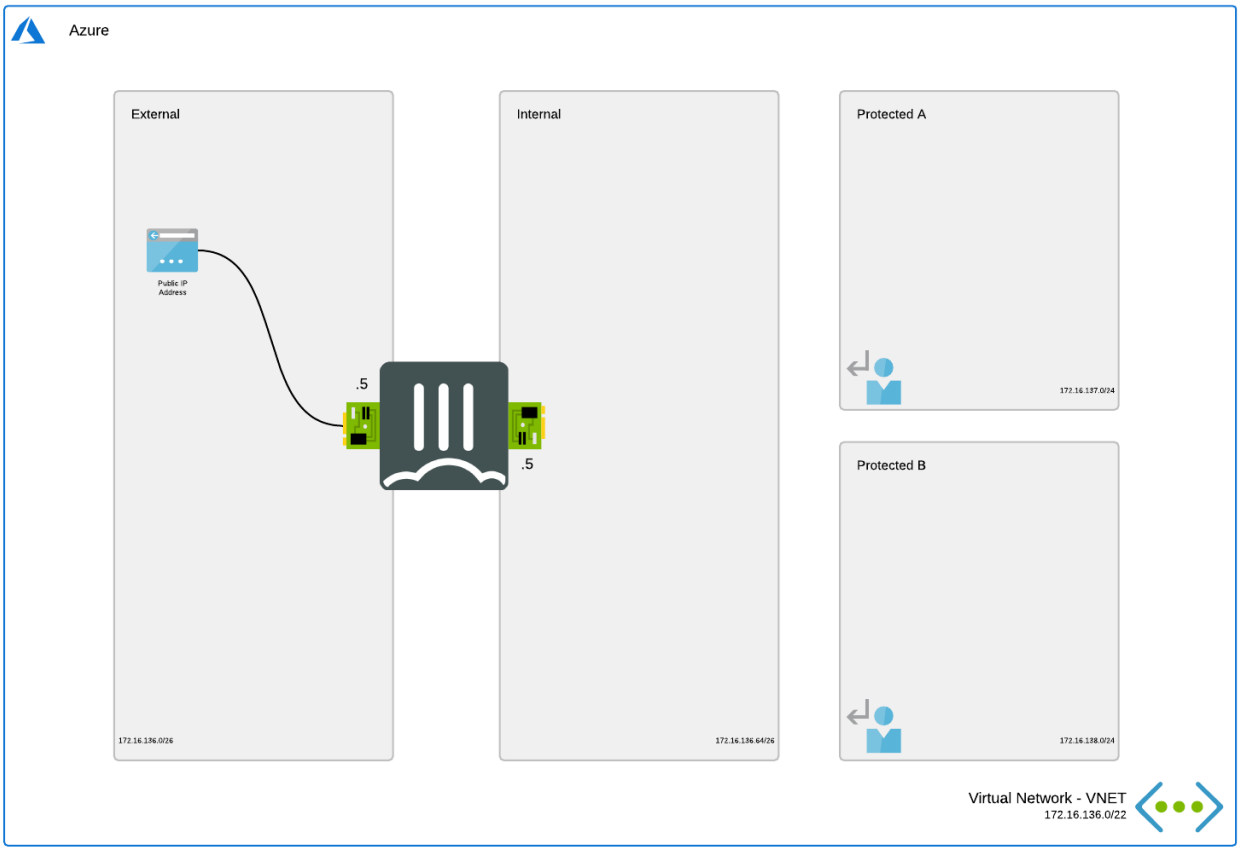
When designing a reliable architecture in Azure, you must take resiliency and high availability (HA) into account. See Reliability quick links. Running the FortiGate next generation firewall inside Azure offers different reliability levels depending on the building blocks that you use.

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

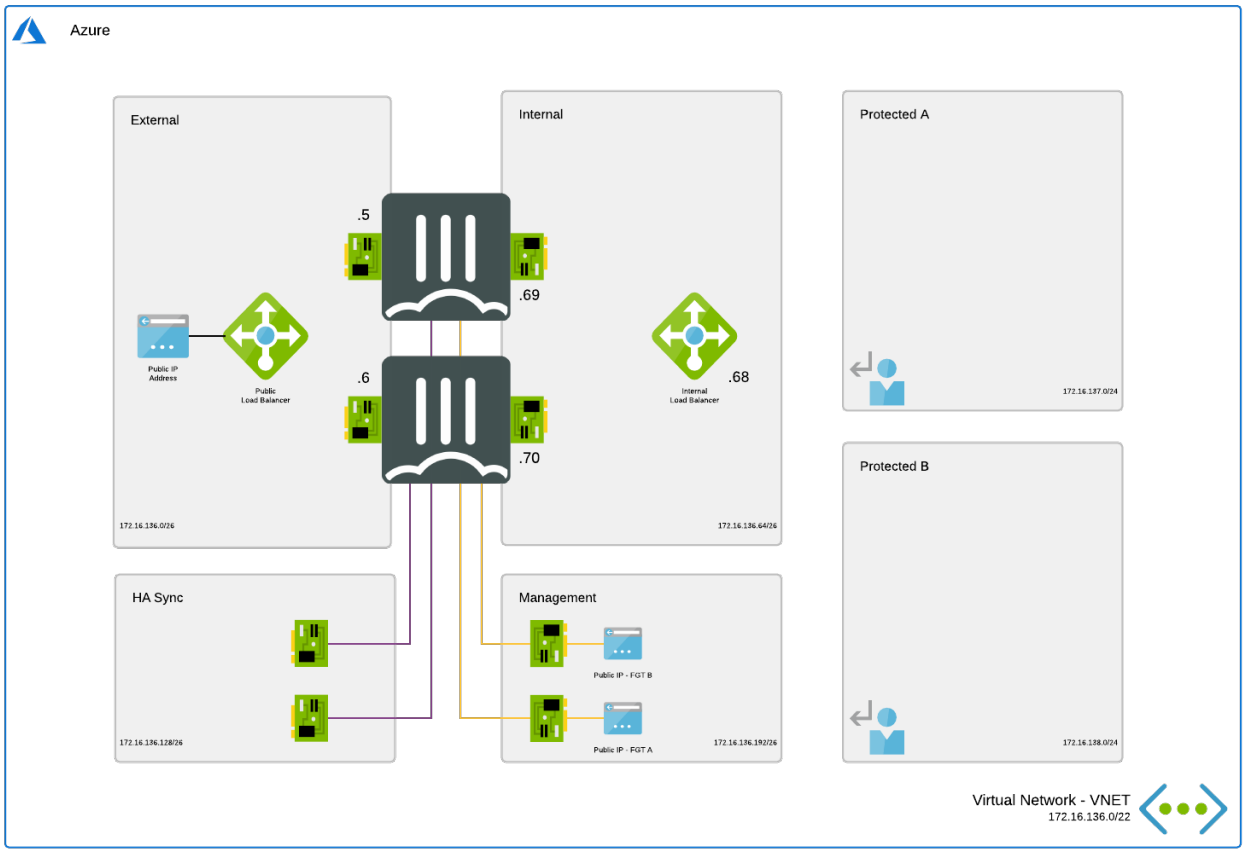
- Availability zone (AZ) (different datacenter in the same region): 99.99%
- Availability set (different rack and power): 99.95%
- Single VM with premium SSD: 99.9%

Building blocks

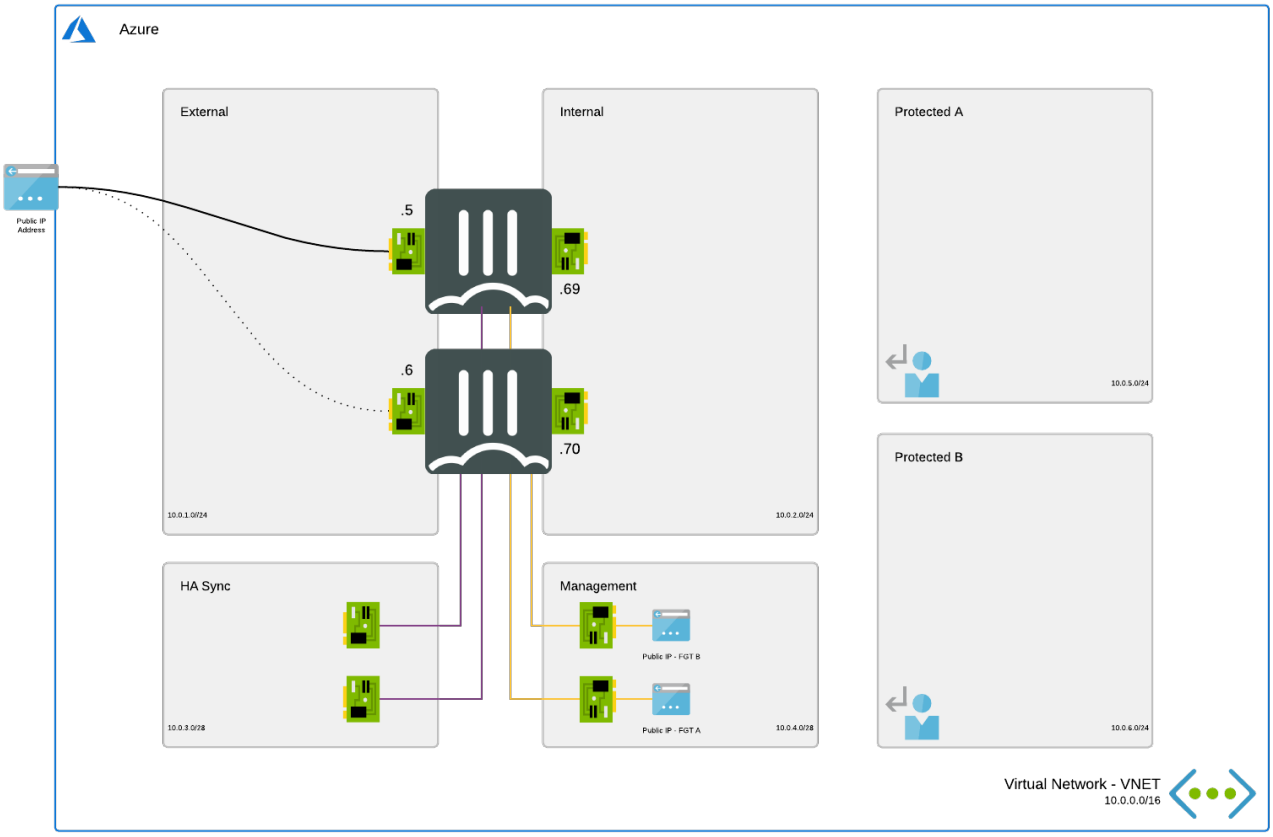
- **Single VM**: this single FortiGate-VM processes all the traffic and becomes a single point of failure during operations and upgrades. You can also use this block in an architecture with multiple regions where a FortiGate is deployed in each region. This setup provides an SLA of 99.9% when using a premium SSD disk. See Single FortiGate-VM deployment on page 134.



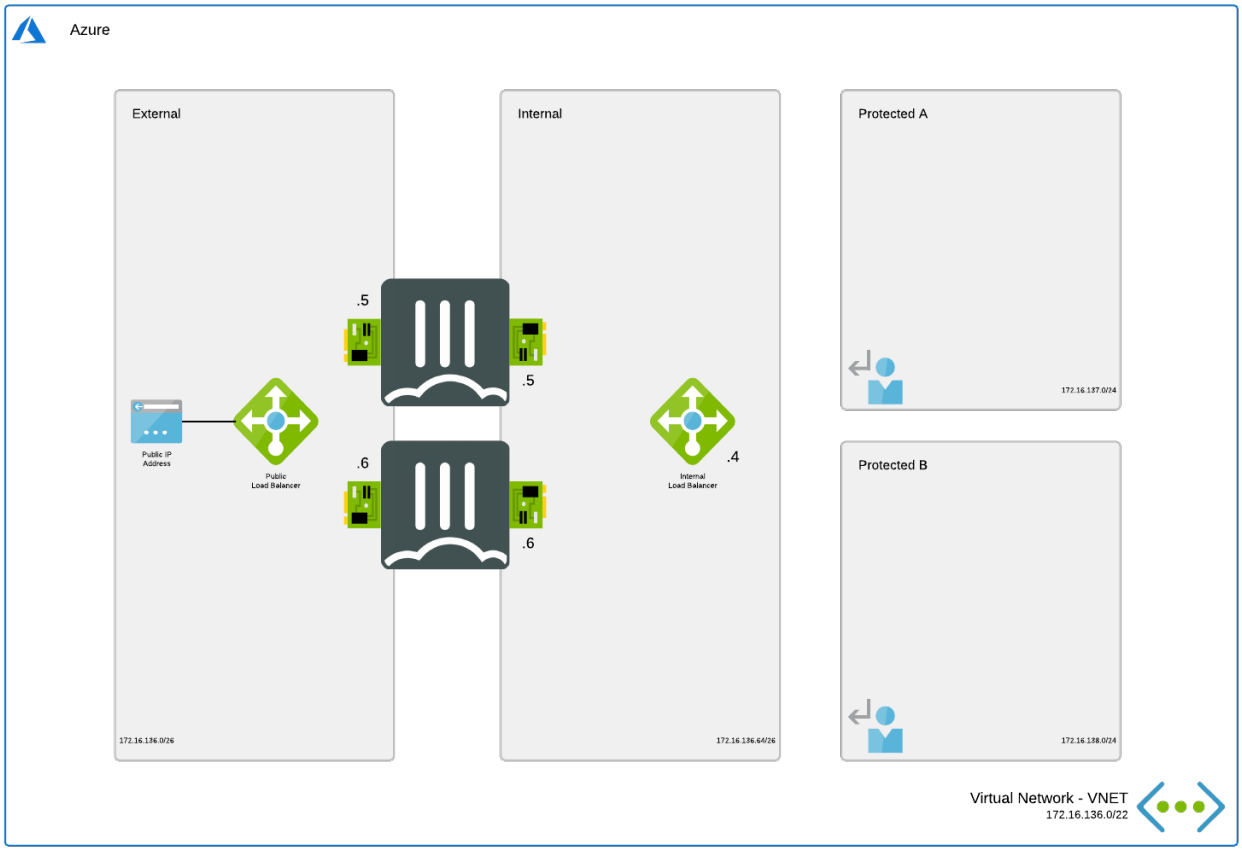
- **Active-passive with external and internal Azure load balancer (LB):** this design deploys two FortiGate-VMs in active-passive mode connected using unicast FortiGate clustering protocol (FGCP) HA protocol. In this setup, the Azure LB handles traffic failover using a health probe towards the FortiGate-VMs. 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 FortiGate. Microsoft provides guidance on this architecture.



- **Active-passive HA with SDN connector failover**: This design deploys two FortiGate-VMs in active-passive mode connected using the unicast FGCP HA protocol. This protocol synchronizes the configuration. On failover, the passive FortiGate 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 FortiGate's case, the API calls logic is built-in instead of requiring additional outside logic like Azure Functions or ZooKeeper nodes.



- **Active-active with external and internal Azure LB:** this design deploys two FortiGate-VMs in active-active as two independent systems. In this setup, the Azure LB handles traffic failover using a health probe towards the FortiGate-VMs. You configure the public IP addresses on the Azure LB. The public IP addresses provide ingress and egress flows with inspection from the FortiGate. You can use a FortiManager or local replication to synchronize configuration in this setup. Microsoft provides guidance on this architecture.



AZs and availability sets are available as options in the Azure marketplace and on the GitHub ARM templates. You can select them during deployment.

Architecture

You can deploy the FortiGate-VM in Azure in different architectures. Each architecture has specific properties that can be advantages or disadvantages in your environment:

Architecture	Description
Single VNet	All building blocks above are ready to deploy in a new or existing VNet. Select your block to get started.
Cloud Security Services Hub (VNet peering)	With VNet peering, you can have different islands deploying different services that different internal and/or external teams manage, while maintaining a single point of control going to on-premise, other clouds, or public Internet. The VNets are connected in a hub-spoke setup where the hub controls all traffic. See VNET-Peering.

In active-passive HA scenarios on Azure, you must set the physical interface IP address (port1) and local tunnel interface IP addresses manually on the secondary FortiGate. HA does not automatically sync these IP addresses. You must also manually copy loopback interface configuration from the HA primary to the secondary FortiGate. Configuring a VDOM exception for "system.interface" does not affect behavior.

Subscribing to the FortiGate-VM

See Deploying FortiGate-VM from the marketplace on page 41.

SDN connector integration with Azure

Configuring an SDN connector in Azure

In this section, you configure FortiGate SDN connector for use with Azure.

In the FortiGate interface, these connectors are called SDN connectors and are SDN connectors that provide integration and orchestration of Fortinet products with key SDN solutions. The Fortinet Security Fabric provides visibility into your security posture across multiple cloud networks, spanning private, public, and Software as a Service (SaaS) clouds. In software-defined networks like Azure, dynamic objects and resources can be cumbersome to secure using traditional firewall policies. By using the SDN connector for use with the Azure IaaS, changes to attributes in the Azure environment can be automatically updated in the Security Fabric. This helps integrate and orchestrate FortiOS IPv4 policies going forward.

Before installing and configuring the Azure SDN connector, the following Azure infrastructure and Fortinet FortiGate-VM components should be in place:

- A valid Azure account and subscription. The account can be one that your organization established or simply one of the free trial options available from Azure. If you do not specify the resource group, you can find all resources that the account has access to.
- You should have a FortiGate-VM deployed in Azure
- An IPv4 outbound policy from the FortiGate-VM on port2 (internal) to port1 (external)
- A VM instance of a resource in the Azure environment

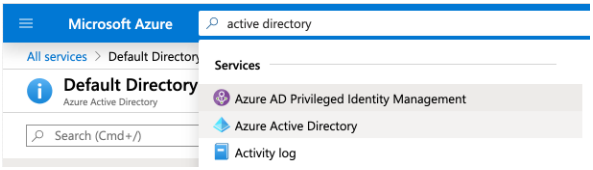
This section describes configuring an Azure SDN connector to connect the FortiGate to connect to the Azure backend. This allows easy reference of dynamic Azure objects when creating FortiOS firewall policies. If the FortiGate is a virtual device in one of those environments, it is likely to be the only connector configured.

Azure SDN connector service principal configuration requirements

To configure an Azure SDN connector using service principal authentication, you must obtain the tenant and client IDs and client secret from the Azure portal.

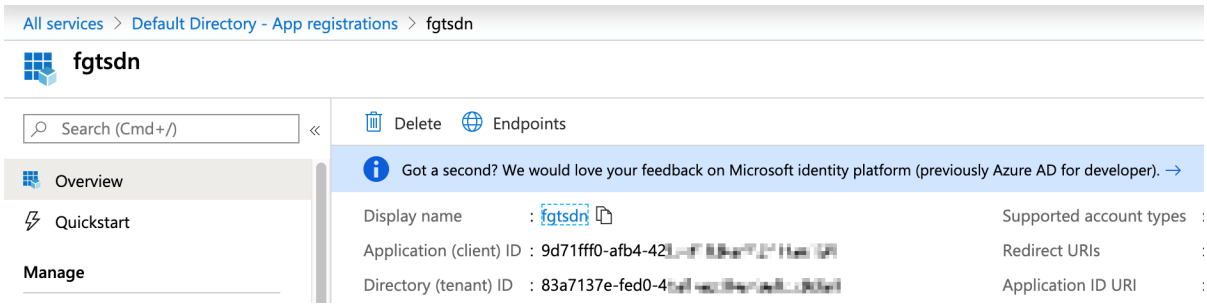
To obtain the tenant and client IDs and client secret:

1. Go to the Azure portal. You can find information required to configure the Azure SDN connector, such as the tenant and client IDs and client secret, in the Azure portal. Find the tenant and client IDs:
   a. In the Azure portal, search for active directory. Click the *Azure Active Directory* service.

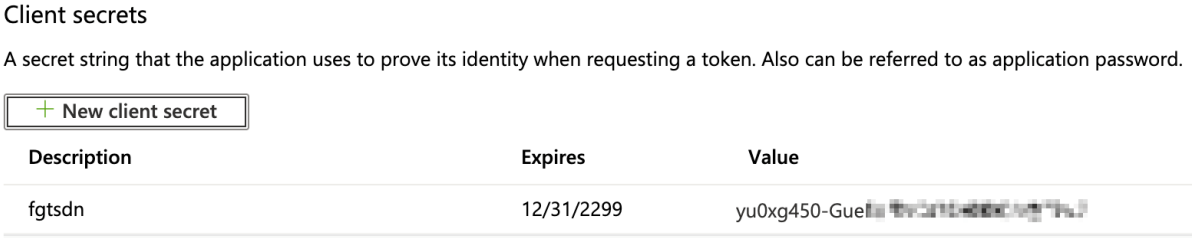


   b. Go to *App registration*.
   c. Click *New registration*.
   d. In the *Name* field, enter the desired name. In this example, the name is fgtsdn.

e. Click *Register*.
f. The overview of the newly created app registration shows the tenant and client ID that the Azure SDN connector requires.



2. Assign a role to the fgtsdn application:
   a. In the Azure portal, search for subscriptions to assign the level of scope to assign this application to.
   b. Click *Pay-As-You-Go*.
   c. Go to *Access control (IAM)*.
   d. Click *Add role assignment*.
   e. From the *Role* dropdown list, select *Contributor*.
   f. In the *Select* field, enter the app name. In this example, it is fgtsdn.
   g. Click *Save*.
3. Generate the client secret value:
   a. Repeat steps 1a-b.
   b. Click the fgtsdn user.
   c. Go to *Certificates & secrets*.
   d. Click the *New client* secret button.
   e. In the *Description* field, enter the desired description.
   f. Under *Expires*, select the desired expiry period.
   g. Click *Add*.
4. Copy the newly created client secret value in to the *Client secret* field in FortiOS.



Configuring an SDN connector using a managed identity

The Azure Active Directory (AD) managed identities for Azure resources feature solves the problem of storing service principal credentials in cloud applications like FortiGate next generation firewall VMs running in Azure.

Instead of authentication using service principal credentials, the SDN connector uses a service principal that the system assigns. The system creates the service principal when you enable managed identities on the VM. Afterward, Azure AD manages the service principal until you destroy the VM.

Configuring a managed identity on Azure

You can enable managed identities on Azure during or after deployment:

- Enabling managed identities on Azure during deployment on page 153
- Enabling managed identities on Azure after deployment on page 153

After deployment, you must give the FortiGate-VM access to Azure resources. See Azure portal on page 155.

Enabling managed identities on Azure during deployment

On the Azure platform, you can enable managed identities from the Azure portal as well as ARM templates during deployment, Azure CLI, PowerShell, or Azure Cloud Shell.

To enable system-assigned managed identities, the Microsoft.Compute/virtualMachines resource for the FortiGate must have the `"identity"` property added at the same level as the`"type": "Microsoft.Compute/virtualMachines"` property.

```
"identity": {
   "type": "SystemAssigned"
},
```

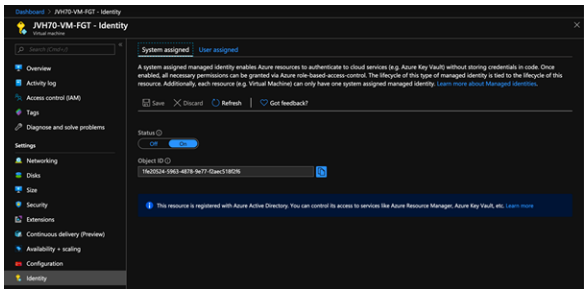
See Configure managed identities for Azure resources on an Azure VM using templates.

Enabling managed identities on Azure after deployment

On a FortiGate previously deployed on Azure, you can enable managed identities using different interaction methods, including the Azure portal, Azure CLI, PowerShell, or a REST API.

Azure portal

The most common method is to use the Azure portal. In the FortiGate-VM resource in the Azure portal, go to *Identity*. On the *System assigned* tab, toggle the *Status* to *On*.



Azure CLI

You can adapt the following command to reflect your VM and resource group names. You can use this command in the Azure CLI installed on Azure Cloud Shell or your local system:

```
az vm identity assign -g myResourceGroup -n myVm
```

See Configure managed identities for Azure resources on an Azure VM using Azure CLI.

Access control

After deployment, you must give the FortiGate-VM access to Azure resources. The SDN connector has two functions:

Function	Description
Dynamic address	The SDN connector can search for private and/or public IP addresses based on different properties, such as tag, VM name, network security group, resource group, and location in the current Azure subscription. You must assign the reader role to the resources that the SDN connector needs access to.
HA	One HA setup includes moving public IP addresses from the active to the passive FortiGate-VM. You must update the user-defined routes to point to the passive FortiGate-VM private IP address. These actions require elevated access to some resources.

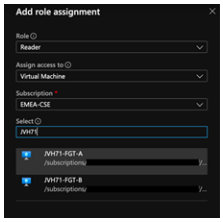
If you want to resolve dynamic addresses in multiple subscriptions in a Cloud Security Services HUB (VNet peering), you must assign the Reader role to each subscription.

Dynamic address

You must assign the Reader role to the whole subscription, as the SDN connector needs access to all resources in the subscription.

To assign access control in the Azure portal:

1. In the Azure portal, go to *Access control (IAM)*.
2. Click *Add a role assignment*.
3. From the *Role* dropdown list, select *Reader*.
4. From the *Assign access to* dropdown list, select *Virtual Machine*.
5. From the *Select* dropdown list, select the desired FortiGate-VM.



To assign access control in the Azure CLI:

You must assign the role to both FortiGate-VMs in an active-active or active-passive setup. You must apply the Reader role since the VM principal ID must be retrieved. This action assigns required access rights for the service principal that Azure AD is managing specific for the FortiGate-VM to access Azure resources in the Azure subscription.

```
$ spID=$(az resource list -n {<FortiGate-VM name>} --query [*].identity.principalId --out
     tsv)
$ az role assignment create --assignee $spID --role 'Reader' --scope /subscriptions/{Azure
     subscription ID}
```

HA

Azure portal

In case of active-passive failover using the SDN connector, the FortiGate-VMs should have write access with the Network Contributor role to the following resources:

- FortiGate-VM network interfaces
- Routing tables that point to the FortiGate-VM internal interface
- Network security group attached to the FortiGate-VM network interface NIC1
- Public IP address attached to the FortiGate-VM network interface NIC1
- VNet or subnet that has the public IP address attached

The Network Contributor access rights are used to update the routing tables and public IP address in case of failover.

To assign access control in the Azure CLI:

For HA, the SDN connector requires additional rights on different Azure resources. You can use the Network Contributor role or a more precise custom role.

You must assign the Fortinet FortiGate SDN Connector RW role to both FortiGate-VMs when in an active-active or active-passive setup. You must apply this role since the VM principal ID must be retrieved. This action assigns required access rights for the service principal that Azure AD is managing specific for the FortiGate-VM to access Azure resources in the Azure subscription.

Create a JSON file that contains the following:

```
{
   "Name": "Fortinet FortiGate SDN Fabric Connector RW",
   "IsCustom": true,
   "Description": "Role to update the public ip addres and user defined routes",
   "Actions": [
      "*/read",
      "Microsoft.Network/routeTables/write",
      "Microsoft.Network/routeTables/routes/write",
      "Microsoft.Network/routeTables/routes/delete",
      "Microsoft.Network/publicIPAddresses/write",
      "Microsoft.Network/publicIPAddresses/join/action",
      "Microsoft.Network/networkInterfaces/write",
      "Microsoft.Network/networkSecurityGroups/join/action",
      "Microsoft.Network/virtualNetworks/subnets/join/action"
   ],
   "DataActions": [],
   "NotActions": [],
   "NotDataActions": [],
   "AssignableScopes": [
      "/subscriptions/{<Azure subscription ID>}"
   ]
}
```

This action assigns required access rights for the service principal that Azure AD is managing specific for the FortiGate-VM to access Azure resources in the Azure subscription.

```
$ az role definition create --role-definition azure_SDN_iamrole_rw.json
$ spID=$(az resource list -n {<FortiGate-VM name>} --query [*].identity.principalId --out
     tsv)
```

```
$ az role assignment create --assignee $spID --role 'Reader' --scope /subscriptions/{Azure
     subscription ID}
```

Configuring the managed identity on the FortiGate-VM

You must enable the SDN connector using the CLI. You do not need to add a tenant ID, client ID, or client key as the connector retrieves these automatically from the Azure instance metadata service.

```
config system sdn-connector
   edit AzureSDN
      set type azure
   end
end
```

Configuring an Azure SDN connector for Azure resources

IP address resolving functionality is available for the following Azure resources:

- VM network interfaces (including VMSS)
- Internet-facing load balancers
- Internal load balancers
- Application gateways

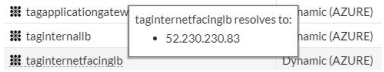
VPN gateways are currently not supported.

The following example demonstrates configuring an internet-facing load balancer.

To configure an internet-facing load balancer address in the GUI:

1. Configure the Azure SDN connector:
   a. Go to *Security Fabric* > *External Connectors*.
   b. Click *Create New*, and select *Microsoft Azure*.
   c. Enter the settings based on your deployment, and click *OK*. The update interval is in seconds.
2. Create the dynamic firewall address:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Click *Create New* > *Address* and enter a name.
   c. Configure the following settings:
      i. For *Type*, select *Dynamic*.
      ii. For *Sub Type*, select *Fabric Connector Address*.
      iii. For *SDN Connector*, select *azure-dev*.
      iv. For *SDN address type*, select *All*.
      v. For *Filter*, enter `Tag.devlb=lbkeyvalue`.
   d. Click *OK*.
      The corresponding IP addresses are dynamically updated and resolved after applying the tag filter.

3. Ensure that the connector resolves the dynamic firewall IP address:
   a. Go to *Policy & Objects* > *Addresses*.
   b. In the address table, hover over the address created in step 2 to view what IP it resolves to:



   c. In Azure, verify to confirm the IP address matches:

To configure an internet-facing load balancer in the CLI:

1. Configure the Azure SDN connector:

```
config system sdn-connector
    edit "azure-dev"
        set status enable
        set type azure
        set azure-region global
        set tenant-id "942b80cd-1b14-42a1-8dcf-4b21dece61ba"
        set client-id "44e79db7-621d-46f3-8625-58e209654e58"
        set client-secret xxxxxxxxxx
        set update-interval 60
    next
end
```

2. Create the dynamic firewall address:

```
config firewall address
    edit "taginternetfacinglb"
        set type dynamic
        set sdn "azure-dev"
        set filter "Tag.devlb=lbkeyvalue"
        set sdn-addr-type all
    next
end
```

   The corresponding IP addresses are dynamically updated and resolved after applying the tag filter.

3. Confirm that the connector resolves the dynamic firewall IP address:

```
config firewall address
    edit "taginternetfacinglb"
        show
            config firewall address
                edit "taginternetfacinglb"
                    set uuid df391760-3bb6-51ea-f775-421df18f368d
                    set type dynamic
                    set sdn "azure-dev"
                    set filter "Tag.devlb=lbkeyvalue"
                    set sdn-addr-type all
                    config list
                        edit "52.230.230.83"
                        next
                    end
```

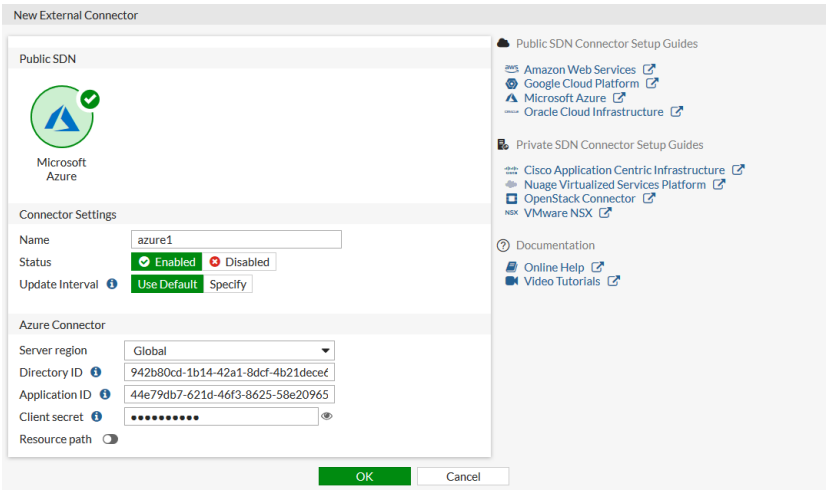
```
                next
            end
        next
end
```

Azure SDN connector using ServiceTag and Region filter keys

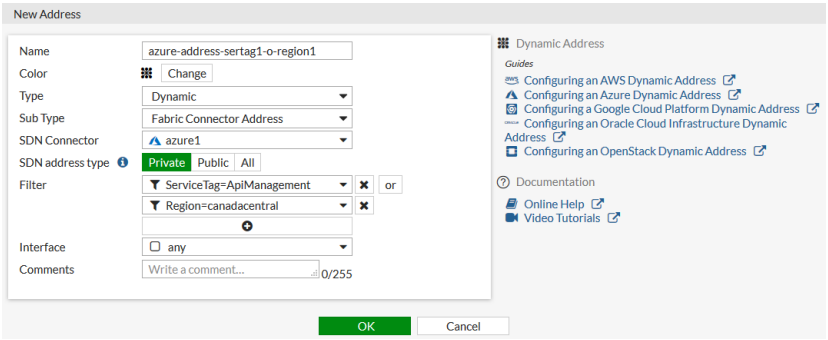
The *ServiceTag* and *Region* filter keys can be used in Azure SDN connectors to filter service tag IP ranges. These can be used in dynamic firewall addresses.

To use the new filters keys in the GUI:

1. Create an Azure SDN connector:
   a. Go to *Security Fabric* > *External Connectors* and click *Create New*.
   b. Select *Microsoft Azure*.
   c. Configure the connector:

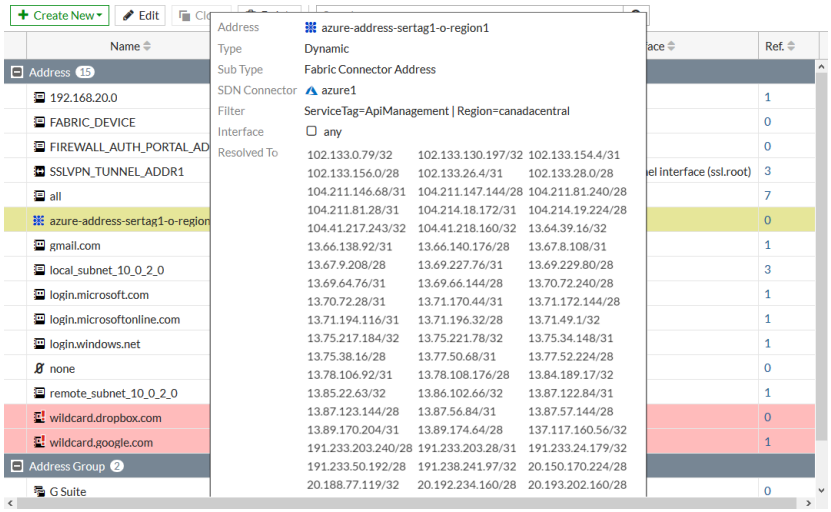


   d. Click *OK*.
2. Create a dynamic firewall address for the Azure connector, filtering based on the servicetag and region:
   a. Go to *Policy & Objects* > *Addresses* and click *Create New* > *Address*.
   b. Configure the address, adding two filters: *ServiceTag=ApiManagement* and *Region=canadacentral*:



   c. Click *OK*.

d. Hover the cursor over the address name to see the dynamic IP addresses that are resolved by the connector:



To use the new filters keys in the CLI:

1. Create an Azure SDN connector:

```
config system sdn-connector
    edit "azure1"
        set type azure
        set tenant-id "942b80cd-1b14-42a1-8dcf-4b21dece61ba"
        set client-id "44e79db7-621d-46f3-8625-58e209654e58"
        set client-secret xxxxxx
    next
end
```

2. Create a dynamic firewall address for the Azure connector, filtering based on the servicetag and region:

```
config firewall address
    edit "azure-address-sertag1-o-region1"
        set type dynamic
        set sdn "azure1"
        set color 2
        set filter "ServiceTag=ApiManagement | Region=canadacentral"
    next
end
```

3. View the dynamic IP addresses that are resolved by the connector:

```
# show firewall address azure-address-sertag1
config firewall address
    edit "azure-address-sertag1"
        set uuid 50a0afd4-b1bf-51ea-651b-f9ba7f6db455
        set type dynamic
        set sdn "azure1"
        set color 2
        set filter "ServiceTag=ApiManagement | Region=canadacentral"
        config list
            edit "102.133.0.79/32"
            next
            edit "102.133.130.197/32"
```

```
                next
                ...
                edit "13.78.108.176/28"
                next
                edit "13.86.102.66/32"
                next
                ...
            end
        next
    end
```

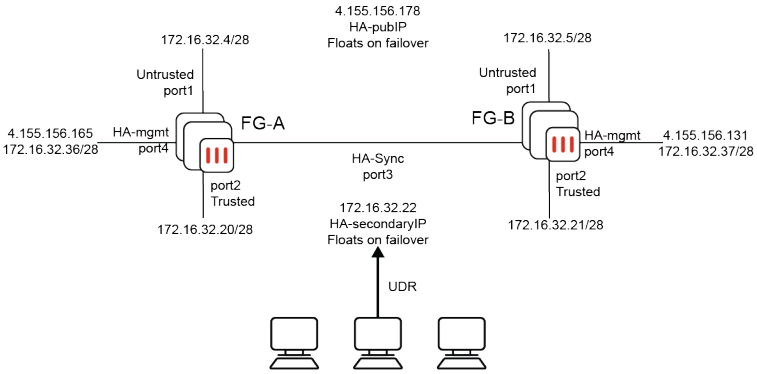
Configuring Azure SDN connector to move private IP address on trusted NIC during A-P HA failover

FortiOS 7.6.1 introduces a floating private IP address on the trusted NIC (port2).

In earlier FortiOS versions, the SDN connector is leveraged to reassociate the public IP address from the old primary instance untrust interface to the new primary instance untrust interface during active-passive high availability (A-P HA) failover and change the next hop to redirect traffic to the new primary instance. In this scenario, you needed to manually update user-defined routes (UDR) to redirect traffic to the new primary instance, which became laborious and difficult to manage.

This feature allows you to avoid manually updating the UDRs after failover. Instead, you can configure all UDRs to use the secondary floating IP address as the next hop. When failover occurs, the SDN connector switches the secondary floating private IP address from the old primary instance to the new primary instance. You can achieve this by deleting the secondary private IP interface and recreating it with the same IP address on the new primary instance. UDRs can remain unchanged. Failover duration depends on the time taken to reassign the private IP address.

The following shows the topology for an example deployment:



The following instructions assume that you have already deployed FortiGate-VMs on Azure as an A-P HA cluster, with the following ports configuration:

Port	Description
port1	untrusted, to_Internet
port2	trusted
port3	HA-sync
port4	HA-mgmt

The SDN connector cannot update the elastic IP address (EIP) without valid authentication. For the SDN connector authentication, you can configure one of the following:

- Azure SDN connector service principal configuration requirements
- Configuring an SDN connector using a managed identity

The following example uses managed identities.

To configure Azure SDN connector to move private IP address on trusted NIC during A-P HA failover:

1. Assign the contributor role to the HA cluster nodes with a scope. See Configure managed identities on Azure virtual machines (VMs):

```
SCOPE="$(az group show -g $RG --query "id" -otsv)"
az vm identity assign --resource-group $RG --role Contributor --scope $SCOPE --name
VNET0-FGT-A
az vm identity assign --resource-group $RG --role Contributor --scope $SCOPE --name
VNET0-FGT-B

{
  "role": "Contributor",
  "scope": "/subscriptions/4f27b38c-ad3f-43d8-a9a3-
01182e5e2f9a/resourceGroups/6899_HA-A",
  "systemAssignedIdentity": "4ae41c9a-146a-415b-b8f8-0a8fdffa6ad8",
  "userAssignedIdentities": {}
}
{
  "role": "Contributor",
  "scope": "/subscriptions/4f27b38c-ad3f-43d8-a9a3-
01182e5e2f9a/resourceGroups/6899_HA-A",
  "systemAssignedIdentity": "9bb34ee6-ae9b-42a1-8d9a-084133ba3b0f",
  "userAssignedIdentities": {}
}
```

2. Verify that the SDN connector is configured and can update the EIP:

```
VNET0-FGT-B (Interim)# get system status
Version: FortiGate-VM64-AZURE v7.6.1,build2686,240806 (interim)
First GA patch build date: 230509
Security Level: 0
Firmware Signature: not-certified
Virus-DB: 1.00000(2018-04-09 18:07)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
AV AI/ML Model: 0.00000(2001-01-01 00:00)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
Proxy-IPS-DB: 6.00741(2015-12-01 02:30)
Proxy-IPS-ETDB: 6.00741(2015-12-01 02:30)
Proxy-APP-DB: 6.00741(2015-12-01 02:30)
FMWP-DB: 24.00071(2024-07-31 17:46)
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
IoT-Detect: 0.00000(2022-08-17 17:31)
```

```
OT-Detect-DB: 0.00000(2001-01-01 00:00)
OT-Patch-DB: 0.00000(2001-01-01 00:00)
OT-Threat-DB: 6.00741(2015-12-01 02:30)
IPS-Engine: 7.00539(2024-05-09 00:34)
Serial-Number: FGTAZRLF5HB4I_03
License Status: Valid
VM Resources: 4 CPU, 7978 MB RAM
Log hard disk: Available
Hostname: VNET0-FGT-B
Private Encryption: Disable
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 2
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, primary
Cluster uptime: 47 minutes, 22 seconds
Cluster state change time: 2024-08-06 12:12:00
Branch point: 2686
Release Version Information: interim
FortiOS x86-64: Yes
System time: Tue Aug  6 12:39:13 2024
Last reboot reason: warm reboot

VNET0-FGT-B (Interim)# show system sdn-connector
config system sdn-connector
    edit "AzureSDN"
        set type azure
        set ha-status enable
        set subscription-id "4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a"
        set resource-group "6899_HA-A"
        config nic
            edit "VNET0-FGT-B-Nic1"
                config ip
                    edit "ipconfig1"
                        set public-ip "HA-A-PIP"
                    next
                end
            next
        end
        config route-table
            edit "VNET0-RouteTable-ProtectedSubnet"
                config route
                    edit "toDefault"
                        set next-hop "172.16.32.21"
                    next
                end
            next
        end
    next
end

VNET0-FGT-B (Interim)# diagnose sys sdn status
SDN Connector                        Type        Status
-------------------------------------------------------------
```

```
AzureSDN                          azure       Up

VNET0-FGT-B (Interim)# execute update-eip
NIC: 172.16.32.5, public IP: 20.191.71.72
NIC: 172.16.32.21
NIC: 172.16.32.37
NIC: 172.16.32.53, public IP: 13.66.252.150
port1: 172.16.32.5, eip: 20.191.71.72
port2: 172.16.32.20
EIP is updated successfully
```

3. On both HA nodes, configure the SDN connector as follows. The commands configure new options, `peer-nic` and `private-ip`:

```
# config for VNET0-FGT-A
#
config system sdn-connector
    edit "AzureSDN"
        config nic
            edit "VNET0-FGT-A-Nic2"
                set peer-nic "VNET0-FGT-B-Nic2"
                config ip
                    edit "ipconfig2"
                        set private-ip "172.16.32.22"
                    next
                end
            next
        end
        config route-table
            edit "VNET0-RouteTable-ProtectedSubnet"
                config route
                    edit "toDefault"
                        set next-hop "172.16.32.22"
                    next
                end
            next
        end
    next
end

# config for VNET0-FGT-B
#
config system sdn-connector
    edit "AzureSDN"
        config nic
            edit "VNET0-FGT-B-Nic2"
                set peer-nic "VNET0-FGT-A-Nic2"
                config ip
                    edit "ipconfig2"
                        set private-ip "172.16.32.22"
```

```
                    next
                end
            next
        end
        config route-table
            edit "VNET0-RouteTable-ProtectedSubnet"
                config route
                    edit "toDefault"
                        set next-hop "172.16.32.22"
                    next
                end
            next
        end
    next
end
```

4. Add a secondary IP address, 172.16.32.22 in this example, to the HA nodes' port2:

```
config system interface
    edit "port2"
        set secondary-IP enable
        config secondaryip
            edit 1
                set ip 172.16.32.22/28
                set allowaccess ping
            next
        end
    next
end
```

5. Run the following in the Azure CLI to associate a secondary IP address to port2:

```
az network nic ip-config create --resource-group $RG \
    --nic-name VNET0-FGT-B-NIC2 --name ipconfig2 \
    --private-ip-address 172.16.32.22
{
  "etag": "W/\"c0249b51-62fe-4524-9676-4b58a167f244\"",
  "id": "/subscriptions/4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a/resourceGroups/6899_
HA-A/providers/Microsoft.Network/networkInterfaces/VNET0-FGT-B-
Nic2/ipConfigurations/ipconfig2",
  "name": "ipconfig2",
  "primary": false,
  "privateIPAddress": "172.16.32.22",
  "privateIPAddressVersion": "IPv4",
  "privateIPAllocationMethod": "Static",
  "provisioningState": "Succeeded",
  "resourceGroup": "6899_HA-A",
  "subnet": {
    "id": "/subscriptions/4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a/resourceGroups/6899_
HA-A/providers/Microsoft.Network/virtualNetworks/VNET0/subnets/InternalSubnet",
    "resourceGroup": "6899_HA-A"
```

```
  },
  "type": "Microsoft.Network/networkInterfaces/ipConfigurations"
}
```

6. Verify the IP configurations on port2 of both nodes:

```
az network nic ip-config list -g $RG  --nic-name VNET0-FGT-B-Nic2
[
  {
    "etag": "W/\"c0249b51-62fe-4524-9676-4b58a167f244\"",
    "id": "/subscriptions/4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a/resourceGroups/6899_
HA-A/providers/Microsoft.Network/networkInterfaces/VNET0-FGT-B-
Nic2/ipConfigurations/ipconfig1",
    "name": "ipconfig1",
    "primary": true,
    "privateIPAddress": "172.16.32.21",
    "privateIPAddressVersion": "IPv4",
    "privateIPAllocationMethod": "Static",
    "provisioningState": "Succeeded",
    "resourceGroup": "6899_HA-A",
    "subnet": {
      "id": "/subscriptions/4f27b38c-ad3f-43d8-a9a3-
01182e5e2f9a/resourceGroups/6899_HA-
A/providers/Microsoft.Network/virtualNetworks/VNET0/subnets/InternalSubnet",
      "resourceGroup": "6899_HA-A"
    },
    "type": "Microsoft.Network/networkInterfaces/ipConfigurations"
  },
  {
    "etag": "W/\"c0249b51-62fe-4524-9676-4b58a167f244\"",
    "id": "/subscriptions/4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a/resourceGroups/6899_
HA-A/providers/Microsoft.Network/networkInterfaces/VNET0-FGT-B-
Nic2/ipConfigurations/ipconfig2",
    "name": "ipconfig2",
    "primary": false,
    "privateIPAddress": "172.16.32.22",
    "privateIPAddressVersion": "IPv4",
    "privateIPAllocationMethod": "Static",
    "provisioningState": "Succeeded",
    "resourceGroup": "6899_HA-A",
    "subnet": {
      "id": "/subscriptions/4f27b38c-ad3f-43d8-a9a3-
01182e5e2f9a/resourceGroups/6899_HA-
A/providers/Microsoft.Network/virtualNetworks/VNET0/subnets/InternalSubnet",
      "resourceGroup": "6899_HA-A"
    },
    "type": "Microsoft.Network/networkInterfaces/ipConfigurations"
  }
]
```

7. In the Azure CLI, verify that the route toDefault next hop IP address is 172.16.32.22:

```
az network route-table route show -g $RG --route-table-name VNET0-RouteTable-
ProtectedSubnet
 --name toDefault
{
  "addressPrefix": "0.0.0.0/0",
  "etag": "W/\"879c8971-1b10-4905-83fd-b63e1c8f76c7\"",
  "hasBgpOverride": false,
  "id": "/subscriptions/4f27b38c-ad3f-43d8-a9a3-01182e5e2f9a/resourceGroups/6899_HA-
A/providers/Microsoft.Network/routeTables/VNET0-RouteTable-
ProtectedSubnet/routes/toDefault",
  "name": "toDefault",
  "nextHopIpAddress": "172.16.32.22",
  "nextHopType": "VirtualAppliance",
  "provisioningState": "Succeeded",
  "resourceGroup": "6899_HA-A",
  "type": "Microsoft.Network/routeTables/routes"
}
```

8. Configure the following so that the endpoint can reach the internet:

```
config firewall policy
    edit 100
        set name "to_Internet"
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end

config firewall vip
    edit "172.16.33.4:80"
        set mappedip "172.16.33.4"
        set extintf "port1"
        set portforward enable
        set extport 80
        set mappedport 80
    next
    edit "172.16.33.4:443"
        set mappedip "172.16.33.4"
        set extintf "port1"
        set portforward enable
        set extport 443
        set mappedport 443
    next
    edit "172.16.33.4:65122"
        set mappedip "172.16.33.4"
```

```
        set extintf "port1"
        set portforward enable
        set extport 65122
        set mappedport 22
    next
    edit "172.16.33.4:69"
        set mappedip "172.16.33.4"
        set extintf "port1"
        set portforward enable
        set protocol udp
        set extport 69
        set mappedport 69
    next
end
config firewall vipgrp
    edit "VIPs_on_Internal"
        set interface "port1"
        set member "172.16.33.4:443" "172.16.33.4:80" "172.16.33.4:65122"
"172.16.33.4:69"
    next
end
config firewall policy
    edit 200
        set name "VIP"
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "VIPs_on_Internal"
        set schedule "always"
        set service "ALL"
    next
end

config system interface
edit root_lo0
set vdom root
set type loopback
end
config firewall policy
    edit 1000
        set srcintf "root_lo0"
        set dstintf "root_lo0"
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set action accept
```

```
            set schedule "always"
            set service "ALL"
            set utm-status enable
            set ssl-ssh-profile "deep-inspection"
            set av-profile "default"
            set webfilter-profile "default"
            set dnsfilter-profile "default"
            set file-filter-profile "default"
            set ips-sensor "default"
            set application-list "default"
        next
    end
```

9. Verify that the endpoint can reach the internet.
10. Trigger HA failover.
11. Verify that the endpoint can reach the internet after failover.

Troubleshooting Azure SDN connector

Output messages may differ depending on your setup.

You can use the `diagnose sys sdn status` command to view the status of your SDN connectors.

You can check if API calls are made successfully by running the following commands in the CLI:

```
diagnose debug enable
diagnose debug application azd -1
```

Open the FortiGate GUI in your browser. Try to disable, then enable the SDN connector.

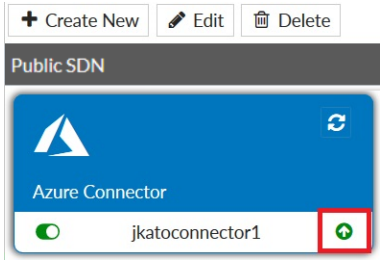
Wait a few minutes. If you did not configure the SDN connector correctly, the CLI displays the following error:

```
jkatofgtha6p-A #
jkatofgtha6p-A # azure sdn connector doing update
getting token
{"error":"invalid_client","error_description":"AADSTS70002: Error valid
get token failed
azd failed to get token
azd failed to get ip addr list
safeguard_fn()-1701
azure sdn connector doing update
getting token
{"error":"invalid_client","error_description":"AADSTS70002: Error valid
get token failed
azd failed to get token
azd failed to get ip addr list
safeguard_fn()-1701
```

Check the following and see if any required configuration is missing or incorrect:

- Did you enter all required fields such as tenant ID, client ID, client secret, subscription ID, and resource groups without error?
- Create a new client secret, then use the new secret for configuration.
- Does the registered app have access to the resource group?

Once you have successfully configured the SDN connector, the indicator turns green and the CLI output no longer shows an error when enabling and disabling the SDN connector.




```
azure sdn connector doing update
getting token
token size:1158
token expire on:1544973259
```

SDN connector in Azure Kubernetes (AKS)

Azure SDN connectors support dynamic address groups based on Azure Kubernetes (AKS) filters. See the *FortiOS Administration Guide*.

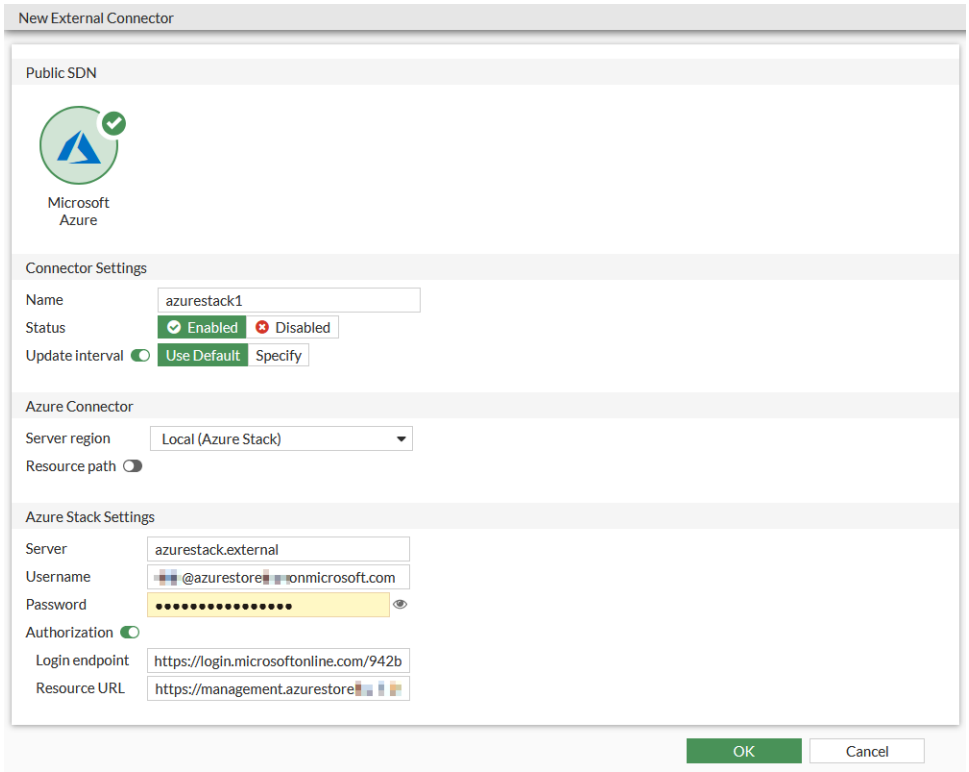
SDN connector in Azure Stack

FortiOS automatically updates dynamic addresses for Azure Stack on-premise environments using an Azure Stack SDN connector, including mapping the following attributes from Azure Stack instances to dynamic address groups in FortiOS:

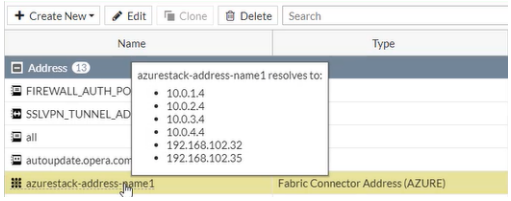
- vm
- tag
- size
- securitygroup
- vnet
- subnet
- resourcegroup
- vmss

To configure Azure Stack SDN connector using the GUI:

1. Configure the Azure Stack SDN connector:
   a. Go to *Security Fabric* > *External Connectors*.
   b. Click *Create New*, and select *Microsoft Azure*.
   c. Configure as shown, substituting the Azure Stack settings for your deployment. The update interval is in seconds.



2. Create a dynamic firewall address for the configured Azure Stack SDN connector:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Click *Create New*, then select *Address*.
   c. Configure the address:
      i. From the Type dropdown list, select *Dynamic*.
      ii. From the *Sub Type* dropdown list, select *Fabric Connector Address*.
      iii. From the *SDN Connector* dropdown list, select the configured Azure Stack connector.
      iv. In the *Filter* field, configure the desired filter. For example, you can configure `vm=tfgta` to automatically populate and update IP addresses only for instances that are named tfgta.
3. Ensure that the Azure Stack SDN connector resolves dynamic firewall IP addresses:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Hover over the address created in step 2 to see a list of IP addresses for instances that are named tftgta as configured in step 2:



To configure Azure Stack SDN connector using CLI commands:

1. Configure the Azure Stack SDN connector:

```
config system sdn-connector
   edit "azurestack1"
      set type azure
      set azure-region local
      set server "azurestack.external"
      set username "username@azurestoreexamplecompany.onmicrosoft.com"
      set password xxxxx
      set log-in endpoint "https://login.microsoftonline.com/942b80cd-1b14-42a1-8dcf-
          4b21dece61ba"
      set resource-url
          "https://management.azurestoreexamplecompany.onmicrosoft.com/12b6fedd-9364-
          4cf0-822b-080d70298323"
      set update-interval 30
   next
end
```

2. Create a dynamic firewall address for the configured Azure Stack SDN connector with the supported Azure Stack filter. In this example, the Azure Stack SDN Connector will automatically populate and update IP addresses only for instances that are named tfgta:

```
config firewall address
   edit "azurestack-address-name1"
      set type dynamic
      set sdn "azurestack1"
      set filter "vm=tfgta"
   next
end
```

3. Confirm that the Azure Stack SDN connector resolves dynamic firewall IP addresses using the configured filter:

```
config firewall address
   edit "azurestack-address-name1"
      set type dynamic
```

```
        set sdn "azurestack1"
        set filter "vm=tfgta"
        config list
           edit "10.0.1.4"
           next
           edit "10.0.2.4"
           next
           edit "10.0.3.4"
           next
           edit "10.0.4.4"
           next
           edit "192.168.102.32"
           next
           edit "192.168.102.35"
           next
        end
     next
  end
```

VPN for FortiGate-VM on Azure

Connecting a local FortiGate to an Azure VNet VPN

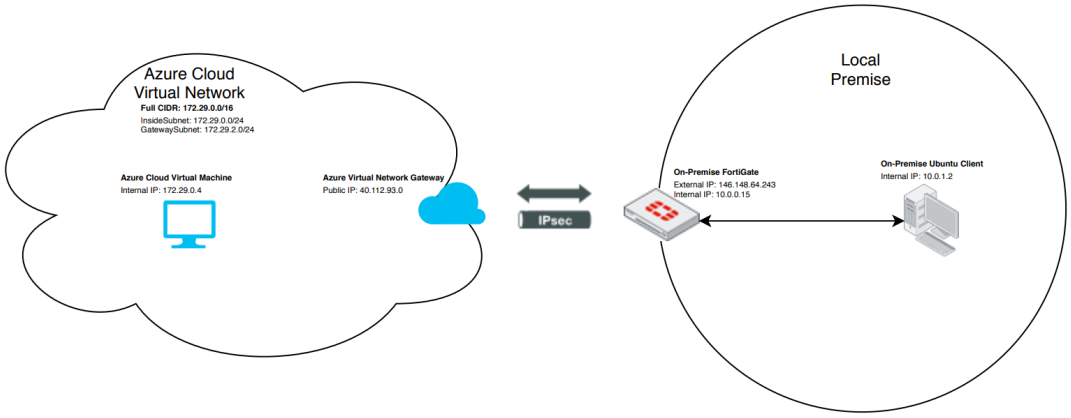
This example provides sample configuration of a site-to-site VPN connection from a local FortiGate to an Azure VNet VPN via IPsec VPN with static or border gateway protocol (BGP) routing.

Instances that you launch into an Azure VNet can communicate with your own remote network via site-to-site VPN between your on-premise FortiGate and Azure VNet VPN. You can enable access to your remote network from your VNet by configuring a virtual private gateway (VPG) and customer gateway to the VNet, then configuring the site-to-site VPC VPN.

The following prerequisites must be met for this configuration:

- Azure VNet with some configured subnets, routing tables, security group rules, and so on
- On-premise FortiGate with an external IP address

The following demonstrates the topology for this example:



This example consists of the following steps:

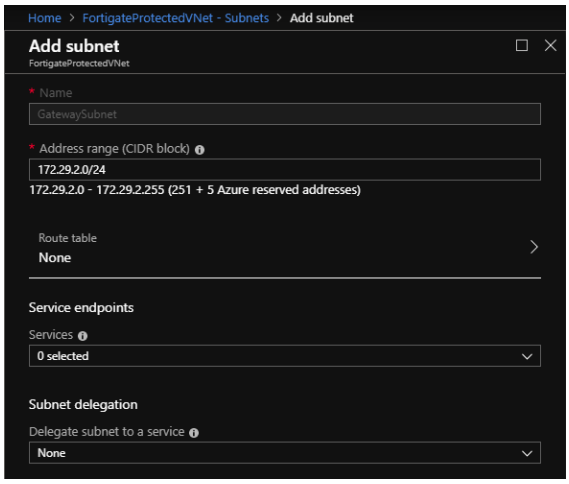
1. Create a gateway subnet.
2. Create a VPN gateway.
3. Create a local network gateway.
4. Create a connection for the VNet gateway.
5. Configure the on-premise FortiGate.
6. Verify the connection.
7. Troubleshoot the connection.

To create a gateway subnet:

A gateway subnet is a subnet in your VNet that contains the IP addresses for the Azure VNet gateway resources and services. Azure requires a gateway subnet for VNet gateways to function.

1. In the Azure management console, go to your VNet, then *Subnets* > + *Gateway subnet*. You do not need to configure any fields on the *Add subnet* screen. You cannot change the name, as it must be GatewaySubnet for the

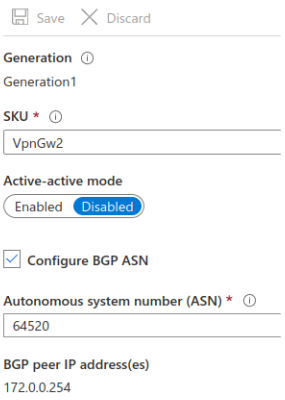
VNet gateway to function. Azure should automatically populate the *Address range (CIDR block)* field with a subnet within your VNet. In this example, the VNet is 172.29.0.0/16, while the subnet is 172.29.2.0/24. You do not need to configure a route table or security group unless your environment needs special handling.



To create a VPN gateway:

You must create a VPN gateway to configure the Azure side of the VPN connection.

1. Go to *Create a resource*. Search for *Virtual network gateway*. Click *Create*.
2. On the *Create virtual network gateway* screen, configure the following:
   a. From the *Subscription* dropdown list, select the correct subscription.
   b. In the *Name* field, enter a name.
   c. From the *Region* dropdown list, select the VNet gateway region. You should select the same region as the VNet.
   d. For *Gateway type*, select *VPN*.
   e. For *VPN type*, select *Policy-based*.
   f. For *SKU*, at the time of publishing this guide, you can only select *Basic* for policy-based VPN.
   g. From the *Virtual network* dropdown list, select the desired VNet to connect to. Azure should automatically detect the gateway subnet created earlier.
   h. Under *PUBLIC IP ADDRESS*, create a new public IP address or select an existing public IP address for the VPN gateway.
   i. If desired, configure BGP. The BGP peer IP address is based on the VNet gateway's gateway subnet.

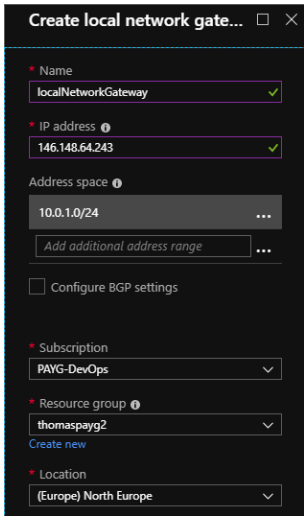


Azure may take up to 45 minutes to create the VPN gateway.

To create a local network gateway:

The local gateway refers to your local side of the VPN settings. You can configure a local network gateway to let Azure know your on-premise-side settings.

1. Go to *Create a resource*. Search for *Local network gateway*. Click *Create*.
2. On the *Create local network gateway* screen, configure the following:
   a. In the *Name* field, enter a name.
   b. In the *IP address* field, enter the on-premise FortiGate's external IP address.
   c. In the *Address space* field, enter the CIDR of the network behind the on-premise FortiGate that will access the Azure VNet.
   d. If desired, enable *Configure BGP settings*. You define the BGP peer IP address for the local network gateway, but there are restrictions. See About BGP with Azure VPN Gateway.
   e. From the *Subscription* dropdown list, select the correct subscription.
   f. From the *Resource group* dropdown list, select the resource group. This example uses the resource group that the other resources belong to.
   g. From the *Location* dropdown list, select the location. This example uses the location that the VNet resides in, but this is not a requirement.



To create a connection for the VNet gateway:

A VNet gateway can have multiple connections to multiple VPN endpoints. These connections share the resource of the VNet gateway. To connect to an on-premise FortiGate, you must configure a connection.

1. Go to the *VNet gateway page* > *Connections* > *Add*.
2. On the *Add connection* screen, configure the following:
   a. In the *Name* field, enter a name.
   b. From the *Connection type* dropdown list, select *Site-to-site (IPsec)*.
   c. Azure should automatically populate and lock the *Virtual network gateway* field.
   d. For *Local network gateway*, select the local network gateway created earlier.
   e. In the *Shared key (PSK)* field, enter the key. You must configure this on the on-premise FortiGate as well.
   f. Azure should automatically populate and lock the *Resource group* field.

To configure the on-premise FortiGate:

On the on-premise FortiGate, you must configure the phase-1 and phase-2 interfaces, firewall policy, and routing to complete the VPN connection. For Azure requirements for various VPN parameters, see Configure your VPN device.

1. Configure the phase-1 interface as follows in the FortiOS CLI:
   a. Set the interface to the external-facing interface.
   b. If your FortiGate is behind NAT, enter the interface's local private IP address for `local-gw`. Otherwise, this step is unnecessary.
   c. For `proposal` and Diffie-Hellman groups, use the ones that Azure supports as Default IPsec/IKE parameters describes.
   d. For the remote gateway, use the VNet gateway's public IP address.
   e. For the PSK secret, use the one configured when creating a connection for the VNet gateway in Azure.
   f. If desired, configure dead peer detection. This is not necessary.

```
config vpn ipsec phase1-interface
   edit "azurephase1"
      set interface "port1"
      set local-gw 10.0.0.15
      set keylife 28800
      set peertype any
      set proposal aes256-sha256 3des-sha1 aes128-sha1 aes256-sha1
      set dhgrp 2
      set remote-gw 40.112.93.0
      set psksecret ENC
           VI0OQ084K91BwEqYp7kzBnMpEfNM1Gg5MnlcTSfxwn4kR5Lsc7QHo0bDAUtqDQMpSrL3bbDBesSxp
           gezyTrlEbzukP5wZHU66uzrG90RARM+f2yZlkEMljw/X3QWl75SAIA4/eSEib3h6M2PqEYvKZf19O
           /tiBihS1ilBM81RblYFI2l2tNLoSatODgRGv8nXkvKVA==
      set dpd-retryinterval 10
   next
end
```

   If configuring BGP routing, also run the following commands. Here, 10.1.254.1 255.255.255.255 is the local network gateway BGP peer IP address. 172.0.0.254 255.255.255.255 is the VNet gateway BGP peer IP address:

```
config system interface
   edit "azurephase1"
      set vdom "root"
      set ip 10.1.254.1 255.255.255.255
      set tcp-mss 1350
      set remote-ip 172.0.0.254 255.255.255.255
   next
end
```

2. Configure the phase-2 interface as follows:
   a. For phase1name, enter the phase-1 interface name as configured in step 1.
   b. For `proposal`, use the ones that Azure supports as Default IPsec/IKE parameters describes.
   c. Disable PFS. Azure does not support it on policy-based mode connections.
   d. You can enable autonegotiation.
   e. Set the key life to 3600 seconds.
   f. Configure the source subnet to the one behind the on-premise FortiGate.
   g. Configure the destination subnet to the Azure VNet's CIDR.

```
config vpn ipsec phase2-interface
   edit "azurephase2"
      set phase1name "azurephase1"
      set proposal aes256-sha1 3des-sha1 aes256-sha256 aes128-sha1
      set pfs disable
```

```
      set auto-negotiate enable
      set keylifeseconds 3600
      set src-subnet 10.0.1.0 255.255.255.0
      set dst-subnet 172.29.0.0 255.255.0.0
   next
end
```

3. Configure ingress and egress firewall policies to the VPN interface:

```
config firewall policy
   edit 1
      set uuid cd18116c-9215-51e9-8398-3398085fff69
      set srcintf "azurephase1"
      set dstintf "port2"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
   next
   edit 2
      set uuid dadd6cd4-9215-51e9-288b-73a4336e9600
      set srcintf "port2"
      set dstintf "azurephase1"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
   next
end
```

4. Configure the route for traffic to enter the VPN tunnel:
   a. Configure a static route for traffic to enter the VPN tunnel:

```
config router static
   edit 1
      set dst 172.29.0.0 255.255.0.0
      set device "azurephase1"
   next
end
```

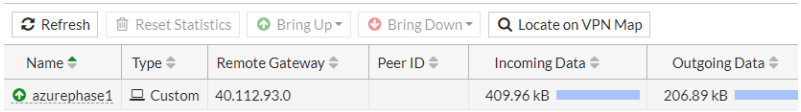
   b. Configure BGP. The example uses the following values:

Value	Description
64521	Local network gateway BGP ASN
172.0.0.254	VNet gateway BGP peer IP address
64520	VNet gateway BGP ASN

```
config router bgp
   set as 64521
   config neighbor
      edit "172.0.0.254"
         set soft-reconfiguration enable
         set remote-as 64520
         set update-source "azurephase1"
      next
   end
end
```

To verify the connection:

1. In FortiOS, go to *Monitor* > *IPsec Monitor* to see if the tunnel is up. If it is not up, manually bring up the tunnel.



2. On the Ubuntu client, conduct a ping test to a resource in the Azure VNet:

```
root@ubuntu-internal:~# ping 172.29.0.4
PING 172.29.0.4 (172.29.0.4) 56(84) bytes of data.
64 bytes from 172.29.0.4: icmp_seq=1 ttl=253 time=101 ms
64 bytes from 172.29.0.4: icmp_seq=2 ttl=253 time=101 ms
64 bytes from 172.29.0.4: icmp_seq=3 ttl=253 time=101 ms
```

3. Verify that the on-premise FortiGate forwards ICMP traffic through the Azure VPN tunnel:

```
EXAMPLE-FGT # diagnose sniffer packet any 'icmp' 4
interfaces=[any]
filters=[icmp]
9.537389 port2 in 10.0.1.2 -> 172.29.0.4: icmp: echo request
9.537453 azurephase1 out 10.0.1.2 -> 172.29.0.4: icmp: echo request
9.638766 azurephase1 in 172.29.0.4 -> 10.0.1.2: icmp: echo reply
9.638800 port2 out 172.29.0.4 -> 10.0.1.2: icmp: echo reply
```

4. If you configured BGP routing, verify the BGP connection between the peers:

```
diagnose sniffer packet azurephase1

interfaces=[azurephase1]

filters=[none]

2.608265 10.1.254.1.3965 -> 172.0.0.254.179: syn 3528484722

2.610865 172.0.0.254.179 -> 10.1.254.1.3965: syn 330055282 ack 3528484723

2.610889 10.1.254.1.3965 -> 172.0.0.254.179: ack 330055283

2.610910 10.1.254.1.3965 -> 172.0.0.254.179: psh 3528484723 ack 330055283

2.616039 172.0.0.254.179 -> 10.1.254.1.3965: psh 330055283 ack 3528484784

2.616051 10.1.254.1.3965 -> 172.0.0.254.179: ack 330055346

2.616061 172.0.0.254.179 -> 10.1.254.1.3965: psh 330055346 ack 3528484784

2.616064 10.1.254.1.3965 -> 172.0.0.254.179: ack 330055365

get router  info bgp summary

BGP router identifier 10.1.1.37, local AS number 64521

BGP table version is 2

2 BGP AS-PATH entries

0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd

172.0.0.254     4      64520    1586    1596        1    0    0 00:01:08        1

Total number of neighbors 1
```

```
get router info routing-table  bgp
Routing table for VRF=0
B       172.0.0.0/16 [20/0] via 172.0.0.254, azurephase1, 00:01:38
```

To troubleshoot the connection:

If any aspects of the VPN are incorrectly configured, you must troubleshoot the Azure and on-premise FortiGate sides.

For Azure-side help, see the Azure documentation.

For the on-premise FortiGate, use debugging to see possible problems:

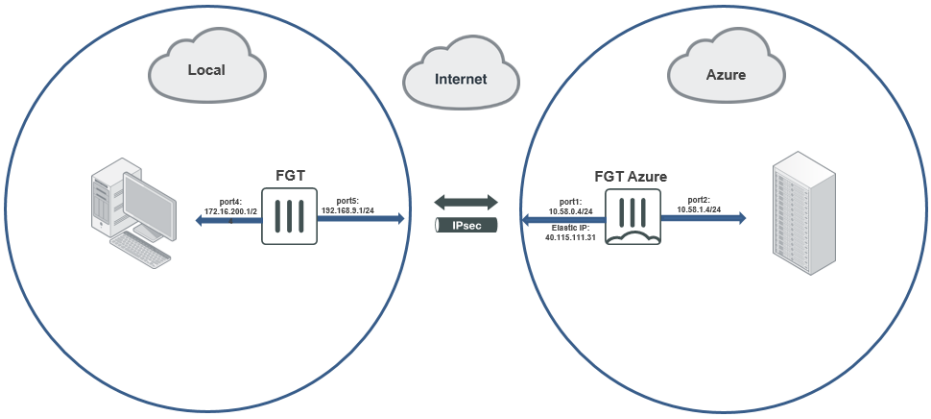
```
EXAMPLE-FGT # diagnose debug enable
EXAMPLE-FGT # diagnose debug application ike -1
Debug messages will be on for 30 minutes.
EXAMPLE-FGT # ike 0: cache rebuild start
ike 0:azurephase1: cached as static-ddns
ike 0: cache rebuild done
ike shrank heap by 106496 bytes
ike 0:azurephase1: NAT keep-alive 3 10.0.0.15->94.245.93.197:4500.
ike 0:azurephase1:125: out FF
ike 0:azurephase1:125: sent IKE msg (keepalive): 10.0.0.15:4500->94.245.93.197:4500, len=1,
     id=ff00000000000000/0000000000000000
ike 0:azurephase1:azurephase2: IPsec SA connect 3 10.0.0.15->94.245.93.197:4500
ike 0:azurephase1:azurephase2: using existing connection
ike 0:azurephase1:azurephase2: config found
ike 0:azurephase1:azurephase2: IPsec SA connect 3 10.0.0.15->94.245.93.197:4500 negotiating
```

Common issues include misconfiguring the local gateway parameter, mismatching security proposals and protocols, and mismatching phase-2 source and destination subnets.

Connecting a local FortiGate to an Azure FortiGate via site-to-site VPN

This guide provides a sample configuration of a site-to-site VPN connection from a local FortiGate to an Azure FortiGate via site-to-site IPsec VPN with static routing.

The following shows the topology for this sample configuration:



This topology consists of the following:

- A local FortiGate is located in a local environment. Determine if your FortiGate has a publicly accessible IP address or if it is behind NAT. In this sample configuration, the local FortiGate is behind NAT.
- A FortiGate located in Azure with port1 connected to WAN and port2 connected to local LAN.

This recipe consists of the following steps:

1. Configure the local FortiGate:
   a. Configure the interfaces.
   b. Configure a static route to connect to the Internet.
   c. Configure IPsec VPN.
2. Configure the Azure FortiGate:
   a. Configure the interface.
   b. Configure IPsec VPN.
3. Bring up the VPN tunnel on the local FortiGate.
4. Verify the VPN tunnel on both the local FortiGate and the Azure FortiGate.
5. Run diagnose commands.

Configuring the local FortiGate

To configure the interfaces:

To configure the interfaces using the GUI, do the following:

1. In FortiOS on the local FortiGate, go to *Network* > *Interfaces*.
2. Edit *port5*. Set the role to *WAN* and set an *IP/Network Mask* of 192.168.5.1/255.255.255.0. This is for the interface connected to the Internet.
3. Edit *port4*. Set the role to *LAN* and set an *IP/Network Mask* of 172.16.200.1/255.255.255.0. This is for the interface connected to the local subnet.

To configure the interfaces using the CLI, run the following commands:

```
FGTA-1 # show system interface port5
config system interface
   edit "port5"
      set vdom "root"
      set ip 192.168.9.1 255.255.255.0
      set allowaccess ping https ssh
      set type physical
      set lldp-reception enable
      set role wan
      set snmp-index 7
   next
end
FGTA-1 # show system interface port4
config system interface
   edit "port4"
      set vdom "root"
      set ip 172.16.200.1 255.255.255.0
      set allowaccess ping https ssh
      set type physical
      set device-identification enable
      set lldp-transmission enable
```

```
      set role lan
      set snmp-index 6
   next
end
```

To configure a static route to connect to the Internet:

To configure a static route using the GUI, do the following:

1. Go to *Network* > *Static Routes*.
2. Click *Create New*.
3. Set the *Destination* to 0.0.0.0/0.0.0.0.
4. For the *Interface*, select *port5*.
5. Set the *Gateway Address* to 192.168.9.254.

To configure a static route using the CLI, run the following commands:

```
FGTA-1 # show router static
config router static
   edit 1
      set gateway 192.168.9.254
      set device "port5"
   next
end
```

To configure IPsec VPN:

To configure IPsec VPN using the GUI, do the following:

1. Go to *VPN* > *IPsec Wizard*.
2. Configure *VPN Setup*:
   a. Enter the desired VPN name. In the example, this is "to_cloud".
   b. For *Template Type*, select *Site to Site*.
   c. For the *Remote Device Type*, select *FortiGate*.
   d. For *NAT Configuration*, select *This site is behind NAT*. For non dial-up situations where your local FortiGate has a public external IP address, you must choose *No NAT between sites*.
   e. Click *Next*.
3. Configure *Authentication*:
   a. For *Remote Device*, select *IP Address*.
   b. Enter an IP address of 40.115.111.31, which is the Azure FortiGate's port1 public IP address.
   c. For *Outgoing Interface*, select *port5*.
   d. Set the *Authentication Method* to *Pre-shared Key*.
   e. Enter a pre-shared key of 123456.
   f. Click *Next*.
4. Configure *Policy & Routing*:
   a. For *Local Interface*, select *port4*.
   b. FortiOS automatically populates *Local Subnets* with 172.16.200.0/24.
   c. Set the *Remote Subnets* to 10.58.1.0/24, which is the Azure FortiGate's port2 subnet.
   d. For *Internet Access*, select *None*.
   e. Click *Create*.

To configure IPsec VPN using the CLI, run the following commands:

```
FGTA-1 # show vpn ipsec phase1-interface to_cloud
config vpn ipsec phase1-interface
   edit "to_cloud"
      set interface "port5"
      set peertype any
      set net-device enable
      set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
      set comments "VPN: to_cloud (Created by VPN wizard)"
      set wizard-type static-fortigate
      set remote-gw 40.115.111.31
      set psksecret ENC xxxxxx
   next
end
FGTA-1 # show vpn ipsec phase2-interface to_cloud
config vpn ipsec phase2-interface
   edit "to_cloud"
      set phase1name "to_cloud"
      set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
           chacha20poly1305
      set comments "VPN: to_cloud (Created by VPN wizard)"
      set src-addr-type name
      set dst-addr-type name
      set src-name "to_cloud_local"
      set dst-name "to_cloud_remote"
   next
end
FGTA-1 # show router static
config router static
   edit 2
      set device "to_cloud"
      set comment "VPN: to_cloud (Created by VPN wizard)"
      set dstaddr "to_cloud_remote"
   next
   edit 3
      set distance 254
      set comment "VPN: to_cloud (Created by VPN wizard)"
      set blackhole enable
      set dstaddr "to_cloud_remote"
   next
end
FGTA-1 # show firewall policy
config firewall policy
   edit 1
      set name "vpn_to_cloud_local"
      set uuid ef98b6d8-41d9-51e9-20c5-7a31a66dd557
      set srcintf "port4"
      set dstintf "to_cloud"
      set srcaddr "to_cloud_local"
      set dstaddr "to_cloud_remote"
      set action accept
      set schedule "always"
      set service "ALL"
      set comments "VPN: to_cloud (Created by VPN wizard)"
   next
   edit 2
      set name "vpn_to_cloud_remote"
      set uuid ef9b260c-41d9-51e9-cf9c-0a082dc52660
```

```
      set srcintf "to_cloud"
      set dstintf "port4"
      set srcaddr "to_cloud_remote"
      set dstaddr "to_cloud_local"
      set action accept
      set schedule "always"
      set service "ALL"
      set comments "VPN: to_cloud (Created by VPN wizard)"
   next
end
```

Configuring the Azure FortiGate

To configure the interface:

To configure the interface using the GUI, do the following:

1. In FortiOS on the Azure FortiGate, go to *Network* > *Interfaces*.
2. Edit *port2*. Set the role to *LAN* and set an *IP/Network Mask* of 10.58.1.4/255.255.255.0. This is for the interface connected to the Azure local subnet.

To configure the interfaces using the CLI, run the following commands:

```
FGT-Azure # show system interface port2
config system interface
   edit "port2"
      set vdom "root"
      set ip 10.58.1.4 255.255.255.0
      set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response capwap
           ftm
      set type physical
      set snmp-index 2
   next
end
```

To configure IPsec VPN:

To configure IPsec VPN using the GUI, do the following:

1. Go to *VPN* > *IPsec Wizard*.
2. Configure *VPN Setup*:
   a. Enter the desired VPN name. In the example, this is "to_local".
   b. For *Template Type*, select *Site to Site*.
   c. For the *Remote Device Type*, select *FortiGate*.
   d. For *NAT Configuration*, select *This site is behind NAT*. For non dial-up situations where your local FortiGate has a public external IP address, you must choose *No NAT between sites*.
   e. Click *Next*.
3. Configure *Authentication*:
   a. For *Incoming Interface*, select *port1*.
   b. Set the *Authentication Method* to *Pre-shared Key*.
   c. Enter a pre-shared key of 123456.
   d. Click *Next*.

4. Configure *Policy & Routing*:
   a. For *Local Interface*, select *port2*.
   b. FortiOS automatically populates *Local Subnets* with 10.58.1.0/24.
   c. Set the *Remote Subnets* to 172.16.200.0/24, which is the local FortiGate's port4 subnet.
   d. For *Internet Access*, select *None*.
   e. Click *Create*.

To configure IPsec VPN using the CLI, run the following commands:

```
FGT-Azure # show vpn ipsec phase1-interface
config vpn ipsec phase1-interface
   edit "to_local"
      set type dynamic
      set interface "port1"
      set peertype any
      set net-device enable
      set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
      set dpd on-idle
      set comments "VPN: to_local (Created by VPN wizard)"
      set wizard-type dialup-fortigate
      set psksecret ENC xxxxxx
      set dpd-retryinterval 60
   next
end
FGT-Azure # show vpn ipsec phase2-interface
config vpn ipsec phase2-interface
   edit "to_local"
      set phase1name "to_local"
      set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
           chacha20poly1305
      set comments "VPN: to_local (Created by VPN wizard)"
      set src-addr-type name
      set dst-addr-type name
      set src-name "to_local_local"
      set dst-name "to_local_remote"
   next
end
FGT-Azure # show firewall policy
config firewall policy
   edit 1
      set name "vpn_to_local_local"
      set uuid 032b6000-41f4-51e9-acb8-b7e32128bb70
      set srcintf "port2"
      set dstintf "to_local"
      set srcaddr "to_local_local"
      set dstaddr "to_local_remote"
      set action accept
      set schedule "always"
      set service "ALL"
      set comments "VPN: to_local (Created by VPN wizard)"
   next
   edit 2
      set name "vpn_to_local_remote"
      set uuid 0343ee4a-41f4-51e9-a06a-d4a15d35a0a2
      set srcintf "to_local"
      set dstintf "port2"
      set srcaddr "to_local_remote"
```

```
      set dstaddr "to_local_local"
      set action accept
      set schedule "always"
      set service "ALL"
      set comments "VPN: to_local (Created by VPN wizard)"
      next
end
```

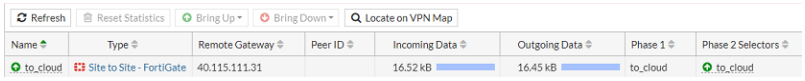
To bring up the VPN tunnel on the local FortiGate:

The tunnel is down until you initiate connection from the local FortiGate.

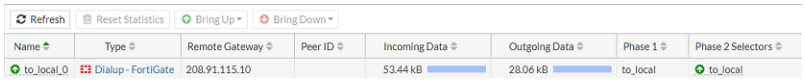
1. In FortiOS on the local FortiGate, go to *Monitor* > *IPsec Monitor*.
2. Click the to_cloud tunnel.
3. Click *Bring Up* to bring up the VPN tunnel.

To verify the VPN tunnel on both the local FortiGate and the Azure FortiGate:

1. In FortiOS on the local FortiGate, go to *Monitor* > *IPsec Monitor*. It should look like the following:



2. In FortiOS on the Azure FortiGate, go to *Monitor* > *IPsec Monitor*. It should look like the following:



To run diagnose commands:

1. To show the local FortiGate's VPN status, run the following commands:

```
FGTA-1 # diagnose vpn ike gateway list
vd: root/0
name: to_cloud
version: 1
interface: port5 13
addr: 192.168.9.1:4500 -> 40.115.111.31:4500
created: 1042s ago
nat: me peer
IKE SA: created 1/1 established 1/1 time 400/400/400 ms
IPsec SA: created 1/1 established 1/1 time 130/130/130 ms
   id/spi: 365 cc00c782040e9ec9/e07668adc21bd6a7
   direction: initiator
   status: established 1042-1041s ago = 400ms
   proposal: aes128-sha256
   key: 2793ba055ddab07a-83c804230bffd8de
   lifetime/rekey: 86400/85058
   DPD sent/recv: 00000000/0000000a
FGTA-1 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=to_cloud ver=1 serial=2 192.168.9.1:4500->40.115.111.31:4500 dst_mtu=1500
bound_if=13 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu
     create_dev frag-rfc accept_traffic=1
proxyid_num=1 child_num=0 refcnt=11 ilast=18 olast=58 ad=/0
stat: rxp=1 txp=2 rxb=16516 txb=16450
```

```
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=4500
proxyid=to_cloud proto=0 sa=1 ref=2 serial=1
   src: 0:172.16.200.0/255.255.255.0:0
   dst: 0:10.58.1.0/255.255.255.0:0
   SA: ref=6 options=10226 type=00 soft=0 mtu=1422 expire=42217/0B replaywin=2048
   seqno=3 esn=0 replaywin_lastseq=00000002 itn=0 qat=0
   life: type=01 bytes=0/0 timeout=42903/43200
   dec: spi=394f6923 esp=aes key=16 4ac11dd0916496e2e1edd610d83c7017
   ah=sha1 key=20 8d0c08ab1ed0d96ae29d521ed954a6bcc270f863
   enc: spi=5dc261b2 esp=aes key=16 c1b49a1251aa9bdb8b0ea205a687c794
   ah=sha1 key=20 0693c8988ef609bc410d6024e72e576366b53fef
   dec:pkts/bytes=1/16440, enc:pkts/bytes=2/16602
   npu_flag=03 npu_rgwy=40.115.111.31 npu_lgwy=192.168.9.1 npu_selid=1 dec_npuid=1 enc_
        npuid=1
```

2. To show the Azure FortiGate's VPN status, run the following commands:

```
FGT-Azure # diagnose vpn ike gateway list

vd: root/0
name: to_local_0
version: 1
interface: port1 3
addr: 10.58.0.4:4500 -> 208.91.115.10:64916
created: 1085s ago
nat: me peer
IKE SA: created 1/1 established 1/1 time 270/270/270 ms
IPsec SA: created 1/1 established 1/1 time 140/140/140 ms

   id/spi: 0 cc00c782040e9ec9/e07668adc21bd6a7
   direction: responder
   status: established 1085-1084s ago = 270ms
   proposal: aes128-sha256
   key: 2793ba055ddab07a-83c804230bffd8de
   lifetime/rekey: 86400/85045
   DPD sent/recv: 0000000b/00000000

FGT-Azure # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=to_local ver=1 serial=1 10.58.0.4:0->0.0.0.0:0 dst_mtu=0
bound_if=3 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/528 options[0210]=create_
     dev frag-rfc accept_traffic=1

proxyid_num=0 child_num=1 refcnt=11 ilast=1096 olast=1096 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
------------------------------------------------------
name=to_local_0 ver=1 serial=2 10.58.0.4:4500->208.91.115.10:64916 dst_mtu=1500
bound_if=3 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/976 options
     [03d0]=create_dev no-sysctl rgwy-chg rport-chg frag-rfc accept_traffic=1

parent=to_local index=0
proxyid_num=1 child_num=0 refcnt=14 ilast=38 olast=38 ad=/0
stat: rxp=334 txp=334 rxb=53440 txb=28056
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=11
natt: mode=keepalive draft=32 interval=10 remote_port=64916
```

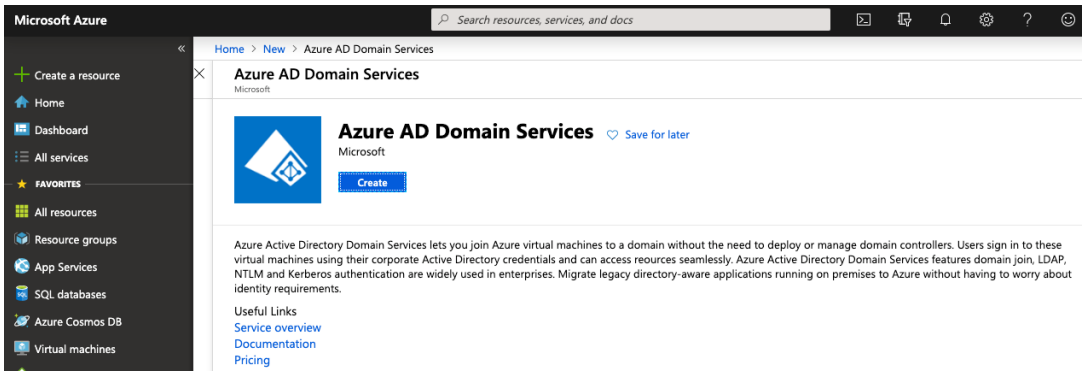
```
proxyid=to_local proto=0 sa=1 ref=2 serial=1 add-route
   src: 0:10.58.1.0/255.255.255.0:0
   dst: 0:172.16.200.0/255.255.255.0:0
   SA: ref=3 options=282 type=00 soft=0 mtu=1422 expire=42460/0B replaywin=2048
   seqno=14f esn=0 replaywin_lastseq=0000014f itn=0 qat=0
   life: type=01 bytes=0/0 timeout=43187/43200
   dec: spi=5dc261b2 esp=aes key=16 c1b49a1251aa9bdb8b0ea205a687c794
   ah=sha1 key=20 0693c8988ef609bc410d6024e72e576366b53fef
   enc: spi=394f6923 esp=aes key=16 4ac11dd0916496e2e1edd610d83c7017
   ah=sha1 key=20 8d0c08ab1ed0d96ae29d521ed954a6bcc270f863
   dec:pkts/bytes=334/28056, enc:pkts/bytes=334/53440
```

Configuring integration with Azure AD domain services for VPN

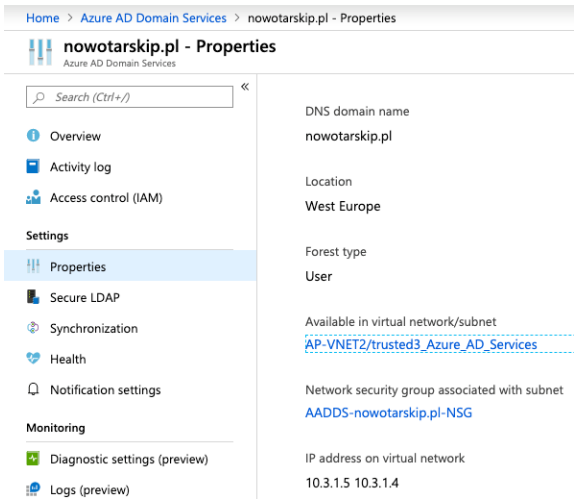
Configuring an integration with Azure AD domain services consists of the following:

To configure Azure AD domain services:

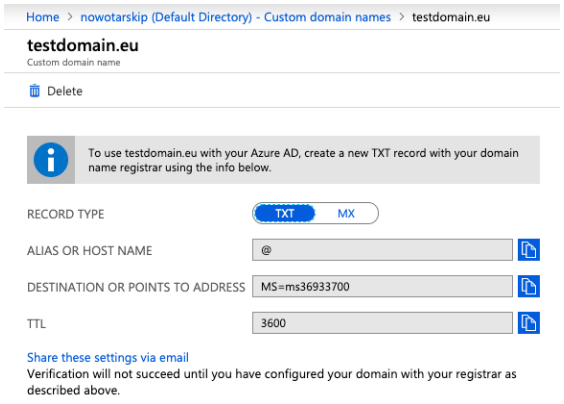
1. In the Azure management portal, create Azure AD domain services. You can deploy it to a new or existing resource group. For information about Azure AD domain services, see Azure AD Domain Services documentation. It can take up to 60 minutes for Azure to create your AD domain.

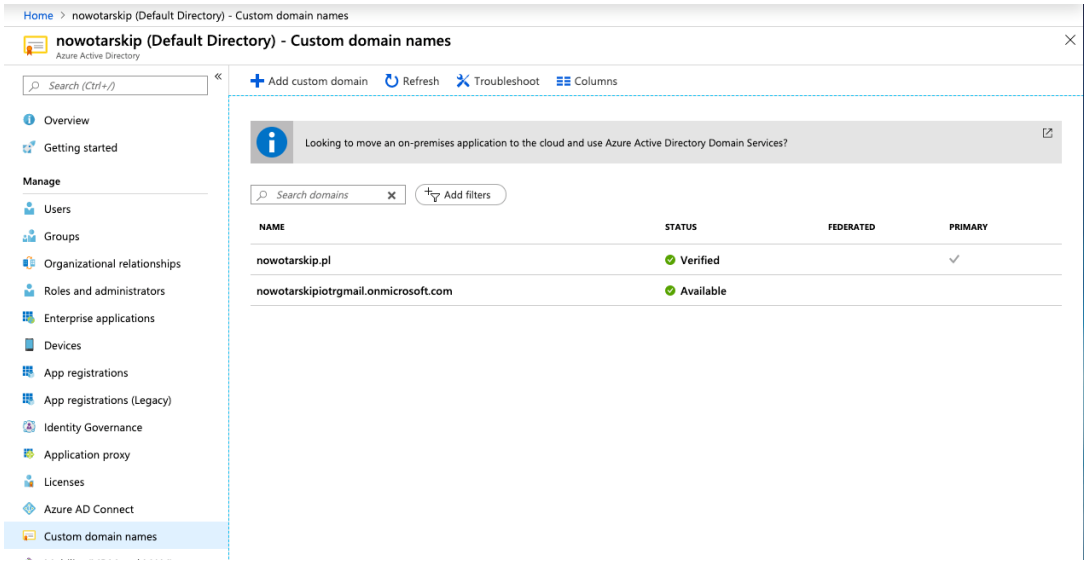


2. Go to *Azure AD Domain Services* > *Synchronization*. Configure whether to synchronize all Azure AD users and groups or scoped groups and members.
3. Go to *Azure AD Domain Services* > *Properties*. You can find IP addresses on which Azure AD domain services are running. These IP addresses must be reachable for your FortiGate for the setup to work.

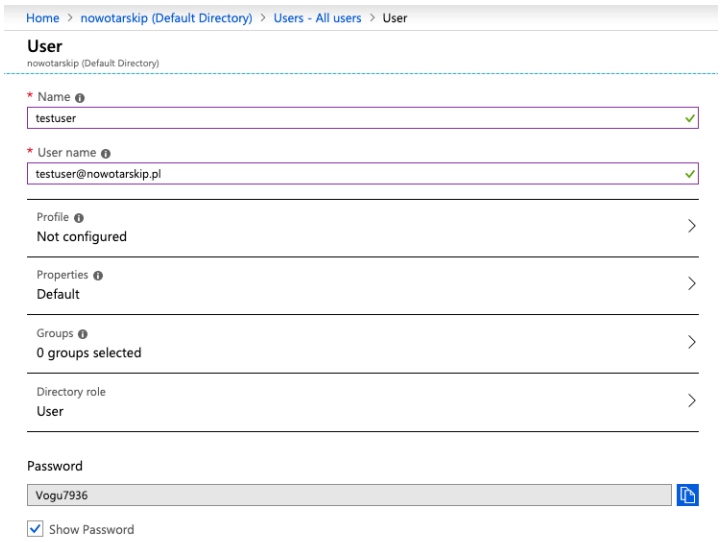


4. Verify your domain in *Azure Active Directory* > *Custom domain names* by adding a TXT or MX record to your DNS settings.

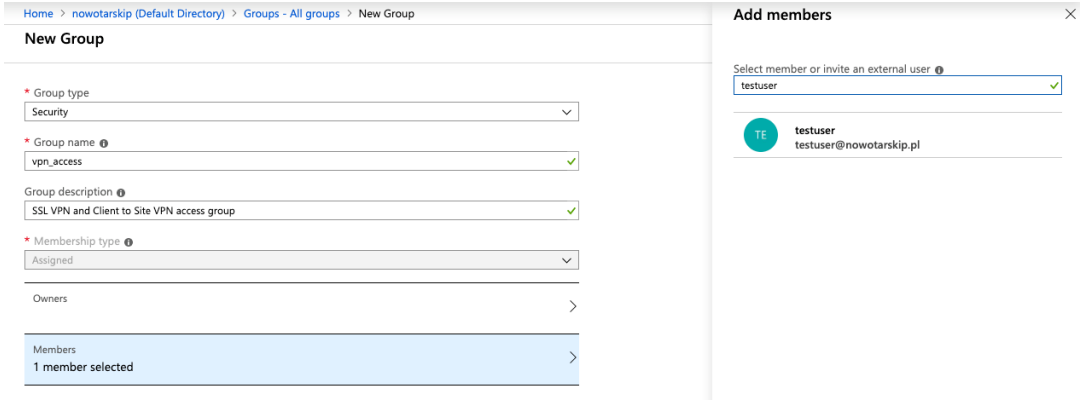




5. Create users in *Azure Active Directory* > *Users* > *New User*. Write down the user password as it is required to log in to https://portal.office.com and you must change the password after initial login.

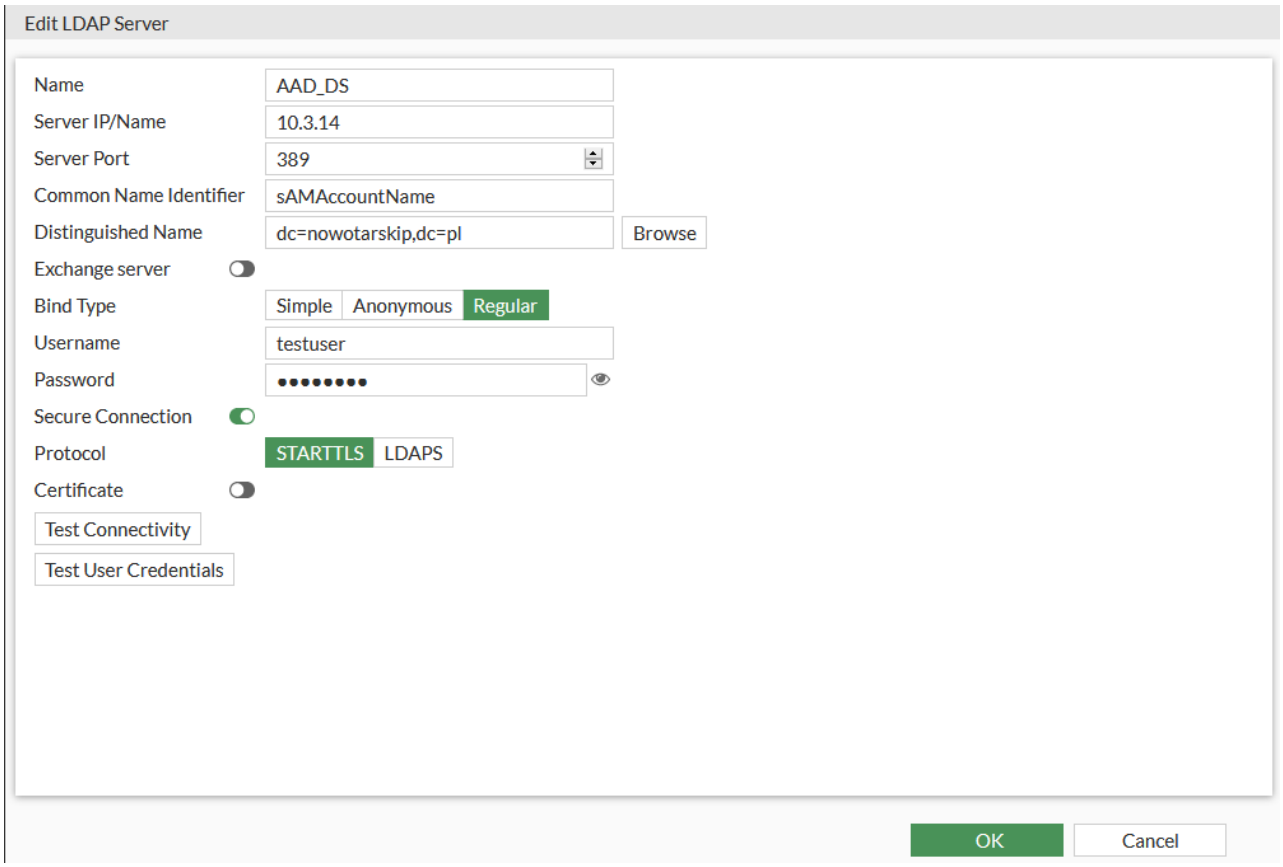


6. In *Azure Active Directory* > *Groups*, create a new group and assign the user created in step 5 to this group.

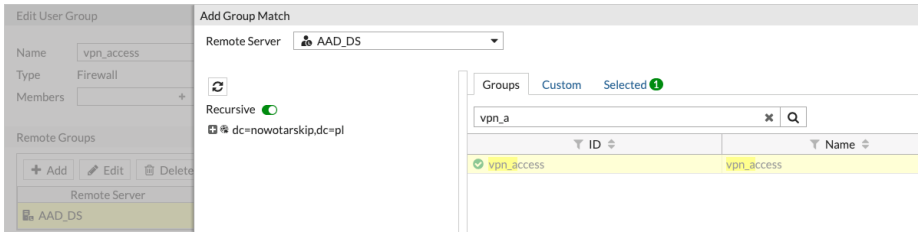


To configure the FortiGate-VM for integration with Azure AD domain services:

1. In FortiOS, go to *User & Authentication* > *LDAP Servers* and configure the LDAP server based on the Azure AD domain service IP address obtained in step 3 of To configure Azure AD domain services: on page 187.



2. Go to *User & Authentication* > *User Groups* and configure the user group that you will be using for the SSL VPN portal or client-to-site VPN connection based on the group that you configured in Azure AD.



3. You can also define a user in *User & Authentication* > *User Definition* that corresponds to the user that you created in step 5 of To configure Azure AD domain services: on page 187. You can use this user in firewall policies for SSL VPN or client-to-site VPN connections.
4. Go to *VPN* > *SSL-VPN Settings* and enable an SSL VPN portal on the WAN interface. See SSL VPN web mode for remote user.

Self-signed certificates are provided by default to simplify initial installation and testing. Acquiring a signed certificate for your installation is **HIGHLY** recommended.

Continuing to use these certificates can result in your connection being compromised, allowing attackers to steal your information, such as credit card details.

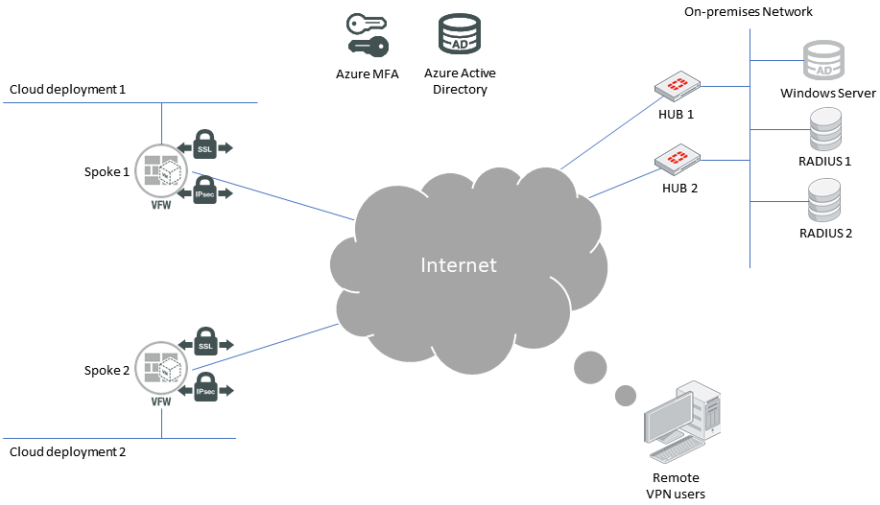
For more information, see Use a non-factory SSL certificate for the SSL VPN portal and learn about Procuring and importing a signed SSL certificate.

5. Go to *Policy & Objects* and edit the SSL VPN policy. For the source, select the user group and/or user that you configured in steps 2 and 3. Define what applications, protocols, and resources to allow for SSL VPN users.

6. Log in to the SSL VPN portal as the Azure AD user.
7. To configure client-to-site VPN access using FortiClient, go to *VPN* > *IPsec Wizard* and select the user group created in step 2. Azure AD creates and manages this group's members. See FortiClient as dialup client for details on configuring FortiClient.
8. You can use Azure AD users as administrator accounts to manage your FortiGate. Go to *System* > *Administrators* and configure a new administrator from a remote server that belongs to the remote user group on Azure AD that you configured in step 2.

Configuring FortiClient VPN with multifactor authentication

This guide outlines how to integrate Azure multifactor authentication (MFA) to existing on-premise and cloud-based user authentication and VPN infrastructure.



This setup consists of the following components:

- On-premise Windows Servers acting as Active Directory (AD) domain controllers with domain name "qa-labs.ca" configured
- Two domain-joined network policy servers (NPS) for RADIUS service
- Cloud-deployed FortiGate-VM spoke nodes with AD VPN connection to the FortiGate-VM hub node for centralized network service accessibility

When a remote VPN user starts FortiClient for VPN connection to any spoke node, the on-premise RADIUS service verifies the user credentials. Integrating Azure MFA to the existing on-premise NPS adds the following MFA methods to the legacy username and password pairs for user authentication:

- Call to phone (wireless or landline phone numbers)
- Text message to phone
- Mobile app token
- Mobile app notification

When the on-premise AD is synced to the Azure AD and NPS extension for Azure is integrated with the NPS, FortiClient VPN authentication flow results, as follows:

1. FortiClient initiates a VPN connection request to the FortiGate-VM with username and password pairs.
2. The FortiGate-VM sends a RADIUS access request message to NPS servers with several attribute value pairs (AVP) parameters, which includes username and encrypted password.
3. The NPS server connects to the local AD for primary authentication for the RADIUS request, if all NPS policies are met.
4. The local AD returns the authentication result to the NPS server. One of the following occurs:
   a. If the credentials are incorrect, the NPS server sends a RADIUS access rejection message to the FortiGate-VM. See step 9.
   b. If the credentials are correct, the NPS server forwards the request to the NPS extension.
5. The NPS extension triggers a request to Azure MFA for secondary authentication. Azure MFA checks if the user has MFA enabled. One of the following occurs:
   a. If the user does not have MFA enabled, go to step 8.
   b. If the user has MFA enabled, go to step 6.
6. Azure MFA retrieves the user details from Azure AD and performs the secondary authentication per the user's predefined methods, such as phone call, text message, mobile app notification, or mobile app one-time password. Azure MFA returns the challenge result to the NPS extension.
7. The NPS server that has the extension installed sends a RADIUS message to the FortiGate-VM. One of the following occurs:
   a. If successful, a RADIUS access accept message is sent. Go to step 8.
   b. If unsuccessful, a RADIUS access reject message is sent. Go to step 9.
8. The user access is granted and an encrypted VPN tunnel is established.
9. The VPN connection from FortiClient is disconnected.

This setup requires the following prerequisites:

- On-premise Windows domain controller and AD
- On-premise RADIUS service provided by NPS
- On-premise FortiGate at center, branch offices with Internet connections
- Azure subscription
- Azure MFA license
- FortiGate-VMon the cloud. Spoke 1 and Spoke 2 have VPN connections to Hub 1 and Hub 2
- Remote VPN users
- Smartphone with Microsoft Authenticator installed

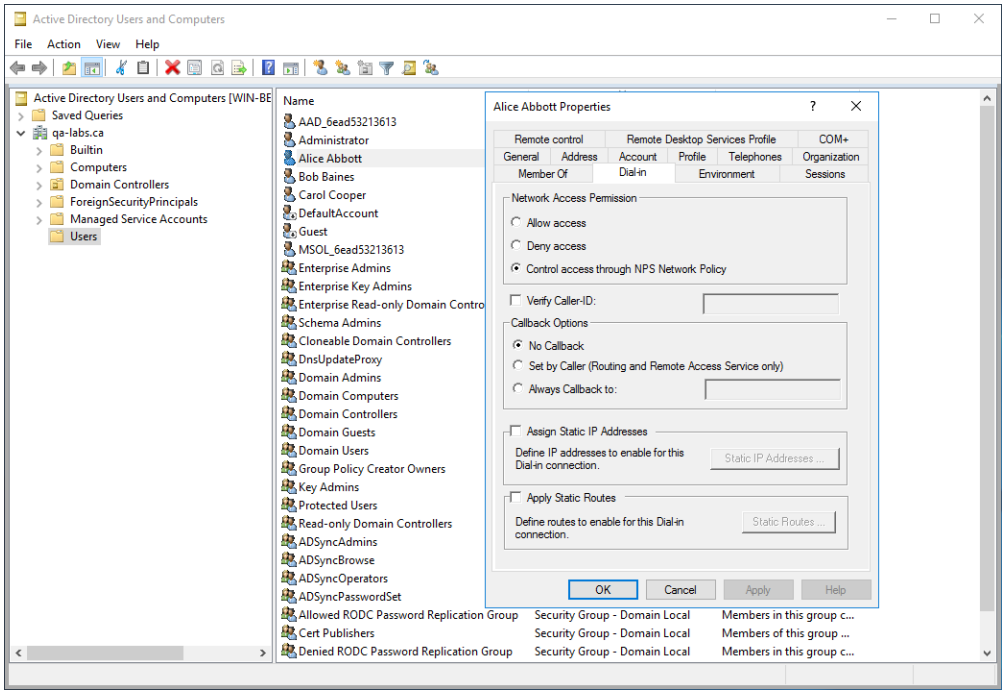
The following example uses the following settings:

- FortiClient 6.0.9
- FortiGate-600D with FortiOS 6.2.2
- FortiGate-VM pay-as-you-go (PAYG) for Azure with FortiOS 6.2.2
- Windows Server 2016, domain controller, domain-joined NPS
- Azure PAYG-DevOps subscription

To configure FortiClient VPN with MFA:

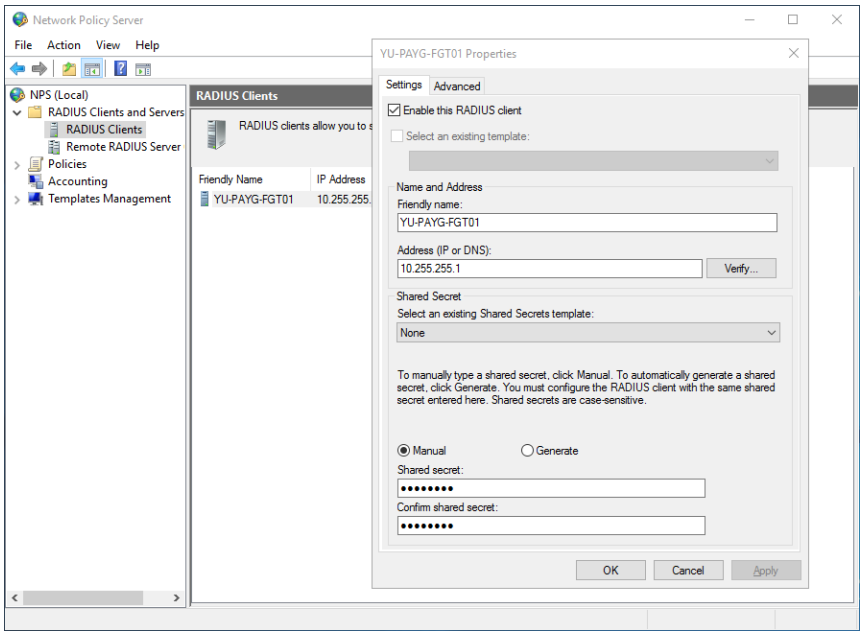
1. Sign in to the Azure portal as a global administrator for the Azure AD. Add your domain name to the Azure AD as a custom domain name so that your users can keep their sign-in username unchanged.
2. Sign in to your on-premise domain controller as the domain administrator. Download and install the Azure AD connect tool to sync your domain users to Azure AD.
3. Download and install the NPS extension to your on-premise NPS server.

4. Add several usernames to your on-premise domain controller for testing purposes. All users should have dial-in control access through NPS network policy under *Network Access Permission*. This example adds the following users:
   - Alice Abbott: aliceabbott@qa-labs.ca
   - Bob Baines: bobbaines@qa-labs.ca
   - Carol Cooper: carolcooper@qa-labs.ca



5. Go to the Azure portal. Click *Azure Active Directory* > *Users* > *Multi-Factor Authentication*. Search and enable MFA for the users you created in step 5.
6. Install Microsoft Authenticator on your smartphone.
7. Sign in to aka.ms/MFASetup as each account that you added in step 5. Enable a different MFA method for each user. This example configures the following:
   - Sign in as Alice Abbott and enable text message.
   - Sign in as Bob Baines and enable mobile app token.
   - Sign in as Carol Cooper and enable mobile app notification.

8. Configure the on-premise NPS:
   a. Add the remote FortiGate-VM as a RADIUS client.



   b. Enable PAP as a RADIUS authentication method.
9. Configure dialup VPN and the SSL VPN portal on the spoke FortiGate-VM with user authenticated against on-premise RADIUS/NPS.

Azure MFA with the RADIUS NPS extension deployment supports the following password encryption algorithms used between the RADIUS client (VPN, NetScaler server, and so on) and the NPS server:

- PAP supports all Azure MFA authentication methods in the cloud: phone call, text, message, mobile app notification, and mobile app verification code.
- CHAPv2 supports phone call and mobile app notifications.
- This deployment does not support EAP.

When FortiOS authenticates a user against a remote RADIUS server, by default, it selects PAP for SSL VPN and MS-CHAPv2 for IPsec VPN. Users who have mobile app token configured as their MFA method may have trouble connecting to IPsec VPN because the mobile app notification or phone call verification may not reach them.

Select PAP for all RADIUS user authentication in your FortiGate-VM configuration:

- For IPsec VPN, run `set xauthtype pap` in your phase1-interface configuration:

```
config vpn ipsec phase1-interface
   edit "Dialup_RAS"
      set type dynamic
      set interface "port1"
      set mode aggressive
      set peertype any
      set net-device disable
      set mode-cfg enable
      set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
      set dpd on-idle
      set comments "VPN: Dialup_RAS (Created by VPN wizard)"
      set wizard-type dialup-forticlient
      set xauthtype pap
      set authusrgrp "Azure_MFA_Usergroup"
```

```
      set ipv4-start-ip 172.31.6.1
      set ipv4-end-ip 172.31.6.254
      set dns-mode auto
      set ipv4-split-include "Dialup_RAS_split"
      set save-password enable
      set client-auto-negotiate enable
      set client-keep-alive enable
      set psksecret Nobody_Knows
      set dpd-retryinterval 60
   next
end
```

- For RADIUS server settings, run `set auth-type pap` and `set timeout 30`:

```
config vpn ssl settings
   set servercert "qa-labs.ca"
   set idle-timeout 4800
   set tunnel-ip-pools "SSLVPN_Tunnel_172.31.7.0/24"
   set source-interface "port1"
   set source-address "all"
   set source-address6 "all"
   set default-portal "web-access"
   config authentication-rule
      edit 1
         set groups "Azure_MFA_Usergroup"
         set portal "0595363 SSLVPN Portal"
      next
   end
end
config user group
   edit "Azure_MFA_Usergroup"
      set member "on-premises_NPS"
   next
end
config user radius
   edit "on-premises_NPS"
      set server "172.31.248.16"
      set secret Nobody_Knows
      set timeout 30
      set nas-ip 10.255.255.1
      set auth-type pap
      set source-ip "10.255.255.1"
   next
end
```

To verify that MFA is configured correctly:

```
diagnose test authserver radius on-premises_NPS pap aliceabbott@qa-labs.ca <password>
Enter Your Microsoft verification code******
authenticate 'aliceabbott@qa-labs.ca' against 'pap' succeeded, server=primary assigned_rad_
     session_id=1070819755 session_timeout=0 secs idle_timeout=0 secs!
diagnose test authserver radius on-premises_NPS pap bobbaines@qa-labs.ca <password>
authenticate 'bobbaines@qa-labs.ca' against 'pap' succeeded, server=primary assigned_rad_
     session_id=1070819758 session_timeout=0 secs idle_timeout=0 secs!
```

Entra ID acting as SAML IdP

Microsoft Entra ID can act as a SAML identity provider (IdP) in the following configurations:

SAML SSO login for FortiOS administrators with Entra ID acting as SAML IdP

See Configuring SAML SSO login for FortiGate administrators with Azure AD acting as SAML IdP.

Configuring SAML SSO login for SSL VPN with Entra ID acting as SAML IdP

This guide provides supplementary instructions on using SAML single sign on (SSO) to authenticate against Microsoft Entra ID with SSL VPN SAML user via tunnel and web modes. You can find the initial Azure configuration in Tutorial: Microsoft Entra SSO integration with FortiGate SSL VPN.

Before you begin the FortiOS configuration, ensure that you collect the following information from Azure to use in the SAML configuration:

FortiGate SAML CLI setting	Equivalent Azure configuration
Service provider (SP) entity ID (`entity-id`)	Identifier (entity ID)
SP assertion consumer service URL (`single-sign-on-url`)	Reply URL (assertion consumer service URL)
SP single logout URL (`single-logout-url`)	Logout URL
Identity provider (IdP) entity ID (`idp-entity-id`)	Microsoft Entra ID identifier
IdP assertion consumer service URL (`idp-single-sign-on-url`)	Azure login URL
IdP single logout URL (`idp-single-logout-url`)	Azure logout URL
IdP certificate (`idp-cert`)	Base64 SAML certificate
Username attribute (`user-name`)	username
Group name attribute (`group-name`)	group

Only a single group claim is allowed in the *User Attributes & Claims* section in Entra ID. You will need to delete the existing group claim and then add a new claim, or you can edit the existing group claim. With this approach, the end result is to change *user.groups* to *All groups* with a custom *Claim Name* of *group*.

Alternatively, you can keep the existing group claim with default settings of *user.groups* set to *Security Groups* with *Claim Name* of *http://schemas.microsoft.com/ws/2008/06/identity/claims/groups*. This is a valid approach using the official claim name specified by Microsoft.

Regardless of the approach chosen, you must ensure that in the FortiGate SAML SSO user settings, the `set group-name` value in the CLI or the *Attribute used to identify groups* in the GUI matches the *Claim Name* specified in the *User Attributes & Claims* section in the Entra ID SAML settings for the FortiGate SSL VPN enterprise application.

To configure SAML SSO:

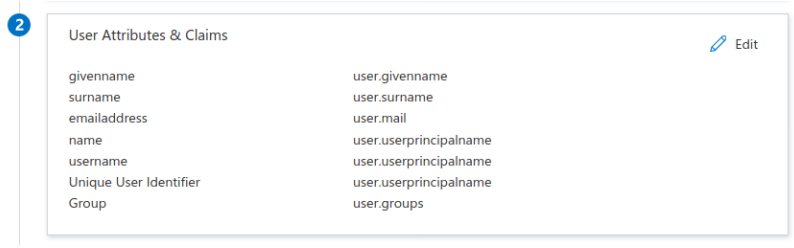
1. In FortiOS, download the Azure IdP certificate as Configure Microsoft Entra SSO describes.
2. Upload the certificate as Upload the Base64 SAML Certificate to the FortiGate appliance describes.
3. In the FortiOS CLI, configure the SAML user.

```
config user saml
   edit "azure"
      set cert "Fortinet_Factory"
      set entity-id "https://<FortiGate IP address or fully qualified domain name
           (FQDN)>:<Custom SSL VPN port>/remote/saml/metadata”
      set single-sign-on-url "https://<FortiGate IP address or FQDN>:<Custom SSL VPN
           port>/remote/saml/login"
      set single-logout-url "https://<FortiGate IP or FQDN address>:<Custom SSL VPN
           port>/remote/saml/logout "
      set idp-entity-id "<Microsoft Entra ID identifier>"
      set idp-single-sign-on-url "<Azure login URL>"
      set idp-single-logout-url "<Azure logout URL>"
      set idp-cert "<Base64 SAML certificate name>"
      set user-name "username”
      set group-name "http://schemas.microsoft.com/ws/2008/06/identity/claims/groups"
   next
end
```

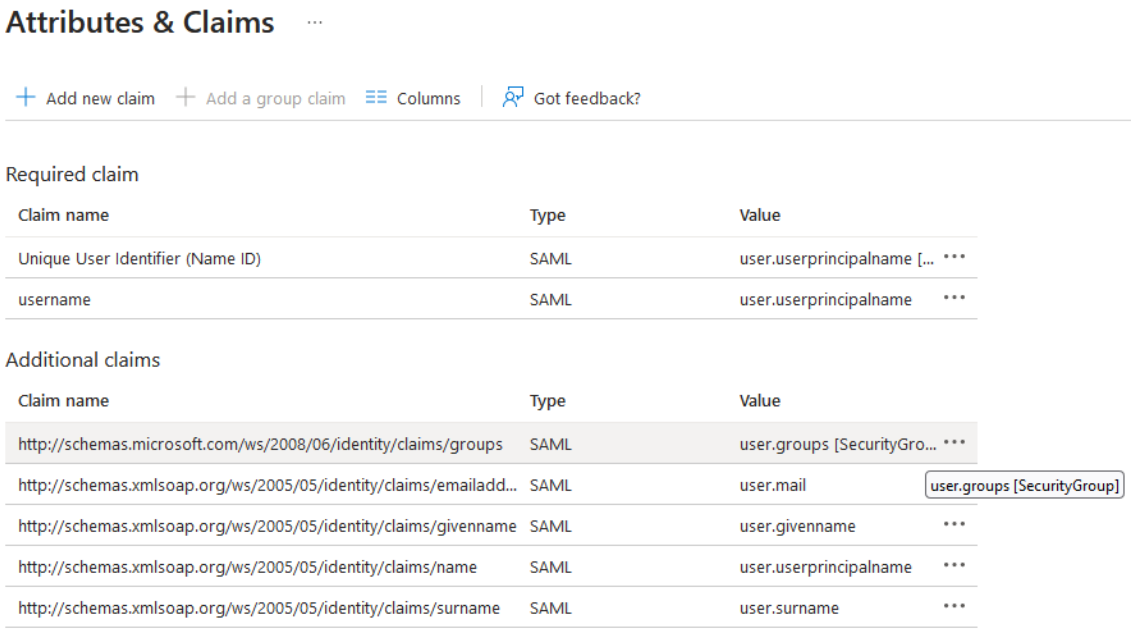
In this example, assuming that the FortiGate IP address is 104.40.18.242, the commands are as follows:

```
config user saml
   edit "azure"
      set cert "Fortinet_Factory"
      set entity-id "https://104.40.18.242:10443/remote/saml/metadata"
      set single-sign-on-url "https://104.40.18.242:10443/remote/saml/login"
      set single-logout-url "https://104.40.18.242:10443/remote/saml/logout"
      set idp-entity-id "https://sts.windows.net/04e..."
      set idp-single-sign-on-url "https://login.microsoftonline.com/xxxxx-xxxxx-xxxxx-
           xxxxx-xxxxx/saml2"
      set idp-single-logout-url "https://login.microsoftonline.com/xxxxx-xxxxx-xxxxx-
           xxxxx-xxxxx/saml2"
      set idp-cert "<Base64 SAML certificate name>"
      set user-name "username"
      set group-name "http://schemas.microsoft.com/ws/2008/06/identity/claims/groups"
   next
end
```

The `user-name` and `group-name` attributes configured on the FortiGate entry should exactly match the username and group attributes that Microsoft Entra ID returns. You can configure the list of SAML attributes that Microsoft Entra ID returns under *Username Attributes & Claims* in the Azure portal.



When you edit the group claim and select *Security groups* as the groups associated with the user that should be returned in the claim, then Azure automatically adds a new claim name in the format http://schemas.microsoft.com/ws/2008/06/identity/claims/groups.



FortiGate can optionally map users to specific groups based on the returned SAML user.groups attribute. The example shows group matching based on Entra ID Group ObjectId, using the `set group-name` command:

```
config user group
   edit FortiGateAccess
      set member azure
      config match
         edit 1
            set server-name azure
            set group-name <object ID>
         next
      end
   next
end
```

You can find the full list of group claims in Configure group claims for applications by using Microsoft Entra ID.

Configure the remote authentication timeout value as needed:

```
config system global
   set remoteauthtimeout 60
end
```

To configure SSL VPN settings:

1. Go to *VPN* > *SSL VPN Settings*. Enable SSL VPN.
2. Configure *Listen on Interface(s)*.
3. Configure the *Listen on Port*. This port should be the port used in the SP URLs in the SAML configurations.
4. Select a server certificate. Fortinet_Factory is used by default. This certificate should match the SP certificate used in the SAML configurations.

Self-signed certificates are provided by default to simplify initial installation and testing. Acquiring a signed certificate for your installation is **HIGHLY** recommended.

Continuing to use these certificates can result in your connection being compromised, allowing attackers to steal your information, such as credit card details.

For more information, see Use a non-factory SSL certificate for the SSL VPN portal and learn about Procuring and importing a signed SSL certificate.

5. Under *Authentication/Portal Mapping*, click *Create New*.
6. Set *Users/Groups* to the user group that you defined earlier. In this example, it is FortiGateAccess.
7. Set *Portal* to the desired SSL VPN portal.
8. Click *OK*.
9. Click *Apply*.

To configure a firewall policy:

1. Go to *Policy & Objects* > *Firewall Policy*. Click *Create new* to create a new SSL VPN firewall policy.
2. Select the incoming and outgoing interfaces. The incoming interface is the SSL VPN tunnel interface (ssl.root).
3. For *Source*, select the SSL VPN tunnel address group and FortiGateAccess user group.
4. Configure other settings as desired.
5. Click *OK*.

To connect in web mode:

1. Go to *https://<FortiGate IP address>:10443* in a browser.
2. Click *Single Sign-On*. The browser redirects to the Azure login portal.
3. Sign in with your Azure account and password. Once logged in, the browser redirects to the SSL VPN portal.

To connect in tunnel mode with FortiClient:

1. In FortiClient, go to *Remote Access*.
2. Add a new connection:
   a. Enter the desired connection name and description.
   b. Set the remote gateway to the FortiGate's fully qualified domain name or IP address.
   c. Enable *Customize port*, then specify the SSL VPN port.
   d. Select *Enable Single Sign On (SSO) for VPN Tunnel*.
   e. (Optional) Enable *Use external browser as user-agent for saml user authentication* if you want users to use their browser session for login.
   f. Click *Save*.
3. Click *SAML Login*. FortiClient redirects the user to the Azure login portal.
4. Sign in with your Azure account and password. Once logged in, the browser redirects to the SSL VPN portal.

To troubleshoot:

```
diagnose debug application samld -1
diagnose debug application sslvpn -1
```

The output should resemble the following:

```
samld_send_common_reply [123]: Attr: 17, 27, magic=a8111ca2943ecd0c
samld_send_common_reply [120]: Attr: 10, 95,
     'http://schemas.microsoft.com/identity/claims/tenantid' 'xxxxx-xxxxx-xxxxx-xxxxx-
     xxxxx'
samld_send_common_reply [120]: Attr: 10, 103,
     'http://schemas.microsoft.com/identity/claims/objectidentifier' 'xxxxx-xxxxx-xxxxx-
     xxxxx-xxxxx'
samld_send_common_reply [120]: Attr: 10, 128,
     'http://schemas.microsoft.com/identity/claims/identityprovider'
     'https://sts.windows.net/xxxxx-xxxxx-xxxxx-xxxxx-xxxxx/'
samld_send_common_reply [120]: Attr: 10, 142,
     'http://schemas.microsoft.com/claims/authnmethodsreferences'
     'http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password'
samld_send_common_reply [120]: Attr: 10, 49, 'Username'
     'mremini@innovcenter.onmicrosoft.com'
samld_send_common_reply [120]: Attr: 10, 51, 'UserGroup' '3a0e3f1c-93c6-4be6-bdbe-
     b5d28a20cfa0'
samld_send_common_reply [120]: Attr: 10, 51, 'UserGroup' '8fb8c5ee-b253-44cc-a88f-
     4bd62dfaf2d2'
[924:root:5c]req: /remote/saml/start
[924:root:5c]rmt_web_auth_info_parser_common:470 no session id in auth info
[924:root:5c]rmt_web_get_access_cache:804 invalid cache, ret=4103
[924:root:5c]sslvpn_auth_check_usrgroup:2039 forming user/group list from policy.
[924:root:5c]sslvpn_auth_check_usrgroup:2145 got user (1) group (1:0).
[924:root:5c]sslvpn_validate_user_group_list:1642 validating with SSL VPN authentication
     rules (0), realm ((null)).
[924:root:5c]sslvpn_validate_user_group_list:1963 got user (1:0), group (1:0) peer group
     (0).
[924:root:0]total sslvpn policy count: 1
[924:root:5c]req: /remote/saml/login
[924:root:5c]stmt: http://schemas.microsoft.com/identity/claims/tenantid
[924:root:5c]stmt: http://schemas.microsoft.com/identity/claims/objectidentifier
[924:root:5c]stmt: http://schemas.microsoft.com/identity/claims/displayname
[924:root:5c]stmt: http://schemas.microsoft.com/identity/claims/identityprovider
[924:root:5c]stmt: http://schemas.microsoft.com/claims/authnmethodsreferences
[924:root:5c]stmt: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
[924:root:5c]stmt: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
[924:root:5c]stmt: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
[924:root:5c]rmt_web_session_create:781 create web session, idx[0]
[924:root:5c]User Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101
     Firefox/71.0
[924:root:5c]deconstruct_session_id:426 decode session id ok, user=[ssl-azure-saml],group=
     [sslvpn],authserver=[],portal=[web-access],host=[208.91.115.10],realm=
     [],idx=0,auth=256,sid=1424c6b9,login=1576802935,access=1576802935,sa$
l_logout_url=no
[924:root:5c]deconstruct_session_id:426 decode session id ok, user=[ssl-azure-saml],group=
     [sslvpn],authserver=[],portal=[web-access],host=[208.91.115.10],realm=
     [],idx=0,auth=256,sid=1424c6b9,login=1576802935,access=1576802935,sa$
l_logout_url=no
[924:root:5c]deconstruct_session_id:426 decode session id ok, user=[ssl-azure-saml],group=
     [sslvpn],authserver=[],portal=[web-access],host=[208.91.115.10],realm=
     [],idx=0,auth=256,sid=1424c6b9,login=1576802935,access=1576802935,sa$
```

```
l_logout_url=no
[924:root:5c]req: /sslvpn/portal.html
[924:root:5c]mza: 0x28587b0 /sslvpn/portal.html
[924:root:5c]deconstruct_session_id:426 decode session id ok, user=[ssl-azure-saml],group=
     [sslvpn],authserver=[],portal=[web-access],host=[208.91.115.10],realm=
     [],idx=0,auth=256,sid=1424c6b9,login=1576802935,access=1576802935,sam
l_logout_url=yes
[924:root:5c]req: /dc7a2776ac5e60eb4eeda4c1de45b5cb/js/req
[924:root:5c]mza: 0x2858620 /dc7a2776ac5e60eb4eeda4c1de45b5cb/js/require_all.js
[924:root:5c]deconstruct_session_id:426 decode session id ok, user=[ssl-azure-saml],group=
     [sslvpn],authserver=[],portal=[web-access],host=[208.91.115.10],realm=
     [],idx=0,auth=256,sid=1424c6b9,login=1576802935,access=1576802935,sam
l_logout_url=yes
[919:root:0]allocSSLConn:289 sconn 0x7f5962887000 (0:root)
total sslvpn policy count: 1
[925:root:0]total sslvpn policy count: 1
[923:root:7b]req: /remote/logout
[923:root:7b]deconstruct_session_id:426 decode session id ok, user=[ssl-azure-saml],group=
     [sslvpn],authserver=[],portal=[web-access],host=[208.91.115.10],realm=
     [],idx=0,auth=256,sid=a205b36,login=1576804178,access=1576804178,saml_logout_url=yes
[923:root:7b]session removed s: 0x7f5962887000 (root)
[923:root:7b]deconstruct_session_id:426 decode session id ok, user=[ssl-azure-saml],group=
     [sslvpn],authserver=[],portal=[web-access],host=[208.91.115.10],realm=
     [],idx=0,auth=256,sid=a205b36,login=1576804178,access=1576804178,saml_logout_url=no
[923:root:0]sslvpn_internal_remove_one_web_session:2848 web session (root:ssl-azure-
     saml:sslvpn:208.91.115.10:0 0) removed for User requested termination of service
[924:root:7a]rmt_check_conn_session:2129 delete connection 0x7f5962887000 w/ web session 0
[924:root:7a]Destroy sconn 0x7f5962887000, connSize=1. (root)
[924:root:7b]rmt_check_conn_session:2129 delete connection 0x7f5962888900 w/ web session 0
[924:root:7b]Destroy sconn 0x7f5962888900, connSize=0. (root)
[923:root:7c]rmt_check_conn_session:2129 delete connection 0x7f5962888900 w/ web session 0
[923:root:7c]Destroy sconn 0x7f5962888900, connSize=1. (root)
[923:root:7b]rmt_check_conn_session:2129 delete connection 0x7f5962887000 w/ web session 0
[923:root:7b]Destroy sconn 0x7f5962887000, connSize=0. (root)
[925:root:7a]SSL state:warning close notify (208.91.115.10)
[925:root:7a]sslConnGotoNextState:305 error (last state: 1, closeOp: 0)
[925:root:7a]Destroy sconn 0x7f5962887000, connSize=1. (root)
dchaofgt # [925:root:7b]SSL state:warning close notify (208.91.115.10)
[925:root:7b]sslConnGotoNextState:305 error (last state: 1, closeOp: 0)
[925:root:7b]Destroy sconn 0x7f5962888900, connSize=0. (root)
```

Azure Sentinel

Sending FortiGate logs for analytics and queries

See Find your Microsoft Sentinel data connector - Fortinet.

Change log

Date	Change description
2024-07-25	Initial release.
2024-09-12	Updated Configuring FGSP session sync on page 86.
2024-09-13	Updated Configuring FGSP session sync on page 86.
2024-10-16	Updated Deploying FortiGate-VM from the marketplace on page 41.
2024-11-28	Added Configuring Azure SDN connector to move private IP address on trusted NIC during A-P HA failover on page 160.

www.fortinet.com