



# FortiNAC

## **Azure Deployment Guide** FortiNAC Version 8.0 and Greater

Date: November 1, 2022

Rev: K

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET KNOWLEDGE BASE**

<https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase>

**FORTINET BLOG**

<http://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<http://support.fortinet.com>

**FORTINET COOKBOOK**

<http://cookbook.fortinet.com>

**NSE INSTITUTE**

<http://training.fortinet.com>

**FORTIGUARD CENTER**

<http://fortiguard.com>

**FORTICAST**

<http://forticast.fortinet.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>



# Contents

Overview .....	4
Requirements .....	4
Considerations.....	5
Build Virtual Machines .....	6
Download the Virtual Appliance.....	6
Prepare the Image.....	8
Prepare an Azure Storage Space and Upload Image .....	9
Determine Memory Allocation.....	9
Create Resource Group and Storage Account .....	9
Upload Prepared VHD Image to Azure .....	10
Create the Virtual Machine .....	14
Serial Console Configuration .....	18
Create Second Network Interface (eth1) .....	19
Add Security Rules .....	20
Configure Subnets Security Rules and Route Tables for eth1 Access .....	20
Assign a Static IP Address .....	20
Appendix .....	21
Install the Azure CLI .....	21
Related Links .....	22

# Overview

This document provides the steps necessary for installing FortiNAC appliance(s). It is intended to be used in conjunction with the [FortiNAC Deployment Guide](#) in the Fortinet Document Library.

For simplicity, this document only discusses the deployment of a FortiNAC virtual appliance with a direct connection to the internet. Other deployment scenarios are possible and more secure. Using a virtual network with a VPN gateway is the preferred deployment. However, those deployments are more involved and beyond the scope of this document.

**Note:** A gateway is required if Azure appliances will be deployed in a High Availability configuration.

**Virtual Appliance (VM) Part Numbers**

Part Number	Description
FNC-M-VM	Control Manager
FNC-CA-VM	Control and Application Server (CA)

## Requirements

- Valid Azure account
- **Note:** There are two sets of commands referenced in this document: Operating system command line and Azure CLI. Operating system command line syntax referenced in this document is based on a computer running the Linux operating system. Windows syntax is not provided.

A Linux computer to prepare and upload the FortiNAC image for Azure. The following must be installed:

- AzureCLI standalone client (see [Appendix](#) for details). The Azure CLI commands in this document are based on Azure CLI version 2.29.1. Exact syntax may vary.
- Qemu (version 2.2.0 or lower, or 2.6 or higher)
- AzCopy
- Gawk
- Sufficient hard drive space (200GB+) available for a fully expanded FortiNAC image
- Either a public or private IP Address can be used. A secure and private topology with FortiNAC is required if a private IP address is used. See [Appendix](#).
- Eth1 isolation related configurations
  - When creating firewall rules for the isolation network, additional MicroSoft IP addresses may need to be allowed. See

<https://www.microsoft.com/en-us/download/confirmation.aspx?id=56519>

- Once FortiNAC is configured, additional domains may have to be added to the Allowed Domains List in order for clients in the isolation network to function properly. For details see [Domains to Add to the Allowed Domains List](#) in the Document Library.
- Note the following when deploying FortiNAC in a High Availability Configuration in Azure:
  - A gateway is required.
  - Both Primary and Secondary Server eth 0 IP's must be on the same subnet for both L2 and L3 HA configurations.
  - A shared/Virtual IP (VIP) cannot be configured in Azure.

## Considerations

- Currently, there is no Azure Market place appliance/product available to quickly deploy a FortiNAC Instance. Instructions are provided to create a disk image.

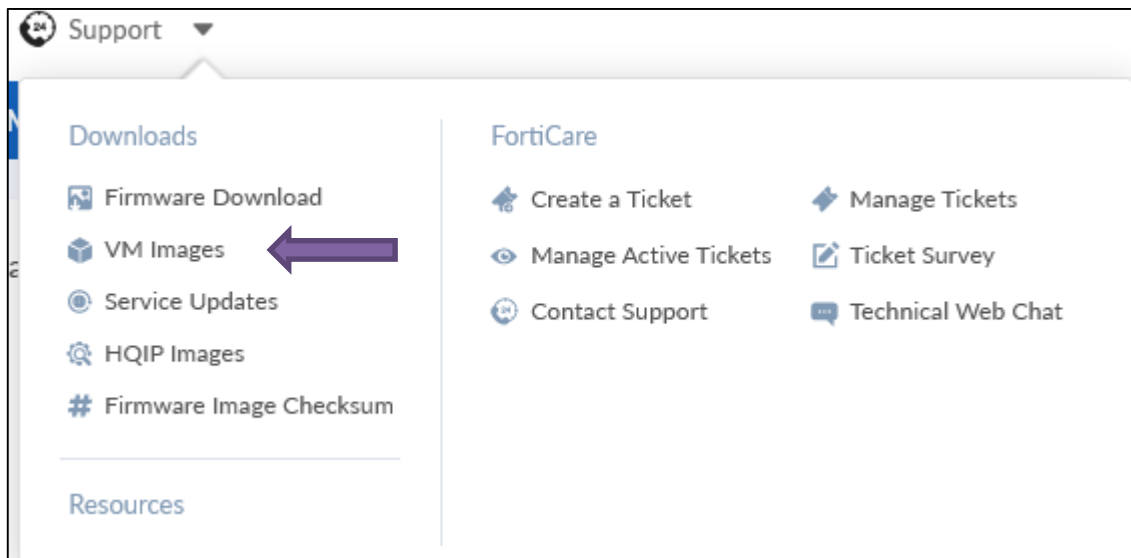
# Build Virtual Machines

## Download the Virtual Appliance

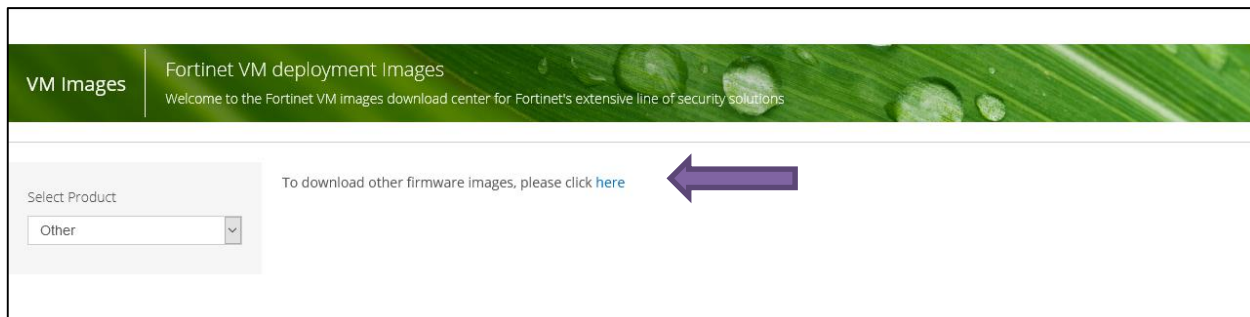
After registering the products, download the appropriate image to the computer running Qemu.

**Note:** Both FortiNAC CA and Manager use the same image. The product type is defined by the license key installed.

1. In the Customer Portal, navigate to **Support > Downloads**
2. Click **VM Images**



3. From drop down list, click **Other** and then click on **here**.



4. From drop down list, select FortiNac.
5. Select the Download Tab to reveal the available versions. Please select the version as recommended by Fortinet or Program Manager.

Note: The suggested version may be the GA version and not the newest version.

6. Click on the file for HyperV (there is no separate image file for Azure).

Example: FNAC\_HyperV\_9.2.1\_build0415.zip

**Firmware Images** | Fortinet Firmware Images And Software Releases

Welcome to the Firmware Images download center for Fortinet's extensive line of security solutions.

**Select Product**

FortiNac ▾





Release Notes | **Download**

**Image File Path**

/ [FortiNac/](#) [v9.00/](#) [9.2/](#) [9.2.1/](#)

**Image Folders/Files**

[Up to higher level directory](#)

	Name	Size (KB)	Date Created	Date Modified	
	FNAC_AWS_9.2.1_build0415.ova	1,129,320	2021-11-05 10:11:43	2021-11-05 10:11:26	<a href="#">HTTPS Checksum</a>
	FNAC_ESX_9.2.1_build0415.ova	1,129,330	2021-11-05 10:11:55	2021-11-05 10:11:51	<a href="#">HTTPS Checksum</a>
	<b>FNAC_HyperV_9.2.1_build0415.zip</b>	1,085,268	2021-11-05 10:11:15	2021-11-05 10:11:42	<a href="#">HTTPS Checksum</a>
	FNAC_install_9.2.1_build0415.bin	164,888	2021-11-05 10:11:26	2021-11-05 10:11:47	<a href="#">HTTPS Checksum</a>

## Prepare the Image

Once the image has been downloaded, convert the VHD image into a RAW disk image and resize it. Azure requires that VHD images have a virtual size aligned to 1MB.

On the computer with the newly downloaded image, perform the following steps from the **operating system command line**.

**Note:** These commands are based on the Linux operating system.

1. Unzip the disk image

```
unzip FNAC_HyperV_9.2.1_build0415.zip
```

2. Convert the VHD to a RAW format. This may take around 3 min.

```
qemu-img convert -O raw fortinac-9.2.1.0415.vhd rawdisk.raw
```

3. Calculate and align to 1MB

```
MB=$((1024*1024))

size=$(qemu-img info -f raw --output json "rawdisk.raw" | \
gawk 'match($0, /"virtual-size": ([0-9]+)/, val) {print val[1]}')
rounded_size=$((($size/$MB + 1)*$MB))

echo "Rounded Size = $rounded_size"
```

4. Resize the RAW disk using \$rounded\_size that was calculated in the previous step

```
qemu-img resize -f raw rawdisk.raw $rounded_size
```

5. Convert the RAW disk back to a fixed-size VHD. This may take around 5 min.

If using qemu version 2.2.0 or lower, use the following command:

```
qemu-img convert -f raw -o subformat=fixed -O vpc rawdisk.raw fortinac-9.2.1.0415_fixed.vhd
```

If using qemu version 2.6+, use the following command:

```
qemu-img convert -f raw -O vpc -o subformat=fixed,force_size rawdisk.raw fortinac-9.2.1.0415_fixed.vhd
```



# Prepare an Azure Storage Space and Upload Image

## Determine Memory Allocation

Determine the appropriate memory allocation for the disk to be created.

### Specifications

Depending on the load, size of the database and whether or not agents are used, there may be a need to increase the amount of memory or number of processors being used. It is recommended the virtual environment be comparable to the physical environment of hardware-based FortiNAC appliances. Refer to the **Specifications** table in the [FortiNAC Data Sheet](#) for details regarding currently shipping hardware.

### Resource Sizing

Virtual Machine settings will vary depending on the underlying hardware being used for the hosting server and the type of FortiNAC server being run in the VM. The ideal result is to yield a VM environment where the average load does not exceed the Total GHz Rating of CPU Resources Allocated. Refer to the **VM Server Resource Sizing** table in the [FortiNAC Data Sheet](#) for suggested memory and CPU requirements.

Note the size in the **Memory** column for the appropriate network size. This will be used when creating the disk in Azure.

## Create Resource Group and Storage Account

Use one of the below options.

### Azure Portal

1. Login to the Azure Portal  
<https://portal.azure.com/>
2. Refer to Microsoft documentation to create a resource group and storage account.
3. Once Created, proceed to [Upload Prepared VHD Image to Azure](#).

### CLI Option: Azure CLI

1. Login to the Azure CLI  
**az login**
2. Create a resource group  
**az group create --name <Resource Group name> --location <Azure region>**

Example

```
az group create --name MyResourceGroup --location eastus
```

3. Create a storage account inside the resource group for the custom disk and VMs

```
az storage account create --resource-group <Resource Group> --location  
<Azure region> -name <storage account name> --kind Storage --sku  
Standard_LRS
```

Example

```
az storage account create --resource-group <Resource Group> --location  
eastus -name myfortinacstorage --kind Storage --sku Standard_LRS
```

4. Create a storage container

```
az storage container create --account-name <storage account name> --  
name <storage container name>
```

Example

```
az storage container create --account-name myfortinacstorage --name  
mydisks
```

5. Proceed to [Upload Prepared VHD Image to Azure](#).

## Upload Prepared VHD Image to Azure

Use one of the below options.

### UI Option: Microsoft Storage Explorer

1. Using Microsoft Storage Explorer, upload the new fixed.vhd file directly to the resource group. Refer to Microsoft documentation for instructions.

<https://docs.microsoft.com/en-us/azure/virtual-machines/disks-use-storage-explorer-managed-disks>

2. Once the disk is uploaded, proceed to [Create the Virtual Machine](#)

## CLI Option: Azure CLI

Reference links:

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/upload-vhd>

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disks-upload-vhd-to-managed-disk-cli>

1. Change the working directory to where the FortiNAC VHD is located. Note the size of the fixed.vhd file (highlighted below). This will be used in a later step.

Example

```
myUser@myUser-mac:/Users/myUser
> cd /Users/myUser/Desktop/MyCompany/AZURE_Cloud_Deployment/FortiNAC
```

```
myUser@myUser-
mac:/Users/myUser/Desktop/MyCompany/AZURE_Cloud_Deployment/FortiNAC
> ls -l
total 17824184
-rw-r--r--@ 1 myUser  staff      1111313665 Nov 10 09:11
FNAC_HyperV_9.2.1_build0415.zip
-rw-r--r--@ 1 myUser  staff      2865616384 Nov  4 13:56 fortinac-
9.2.1.0415.vhd
-rw-r--r--@ 1 myUser  staff    107377328640 Nov 10 11:35 fortinac-
9.2.1.0415_fixed.vhd
-rw-r--r--@ 1 myUser  staff    107377328128 Nov 10 11:34 rawdisk.raw
```

2. Log in to the Azure CLI

**az login**

Example

```
myUser@myUser-
mac:/Users/myUser/Desktop/Fortinet/AZURE_Cloud_Deployment/FortiNAC
> az login
```

The default web browser has been opened at <https://login.microsoftonline.com/common/oauth2/authorize>. Please continue the login in the web browser. If no web browser is available or if the web browser fails to open, use device code flow with `az login --use-device-code`.

You have logged in. Now let us find all the subscriptions to which you have access...

The following tenants don't contain accessible subscriptions. Use 'az login --allow-no-subscriptions' to have tenant level access.

2c36c478-3d00-452f-8535-48396f5f01f0 'Fortinet'

...

3. Create an empty managed disk for the FortiNAC (fixed) VHD. The size of the disk being created needs to be the same size as fixed.vhd file previously created.

```
az disk create -n <disk name> -g <resource group> --os-type Linux --for-upload --upload-size-bytes <fixed disk VHD size> --sku standard_lrs -size-gb <Memory value>
```

#### Example

```
myUser@myUser-  
mac:/Users/myUser/Desktop/MyCompany/AZURE_Cloud_Deployment/FortiNAC  
> az disk create -n fortinac-9.2.1.0415_v4 -g MyResourceGroup --os-type  
Linux --for-upload --upload-size-bytes 107377328640 --sku standard_lrs -  
size-gb <Memory value>
```

...

4. Grant access to this disk so the VHD can be uploaded. Use the following command:

```
az disk grant-access -n <disk name> -g <resource group> --access-level Write  
--duration-in-seconds 86400
```

This command returns a URL that will be used to access the managed disk (highlighted).

#### Example:

```
myUser@myUser-  
mac:/Users/myUser/Desktop/MyCompany/AZURE_Cloud_Deployment/FortiNAC  
> az disk grant-access -n fortinac-9.2.1.0415_v4 -g MyResourceGroup --  
access-level Write --duration-in-seconds 86400  
  
{  
  "accessSas": "https://md-impexp-  
tzjpsd5wdp5p.z15.blob.storage.azure.net/bcgqb1dns1jg/abcd?sv=2018-03-  
28&sr=b&si=f563200f-b90d-45ff-b8ff-  
7970e301a718&sig=bpuyXzF5OyAWBcjzkLFMUZd%2BIEU3a0oOWS0Arq4tqoM%3D"  
}
```

5. Copy the VHD to the managed disk with the command (use double quotes around the URL.):

```
azcopy copy <fixed.vhd filename> "<accessSas URL>" --blob-type PageBlob
```

**Note:** This command may take some time to complete depending on the internet connection.

## Example

```
myUser@myUser-  
mac:/Users/myUser/Desktop/MyCompany/AZURE_Cloud_Deployment/FortiNAC  
> azcopy copy fortinac-9.2.1.0415_fixed.vhd "https://md-impexp-  
tzjpsd5wdp5p.z15.blob.storage.azure.net/bcgqblDNSljg/abcd?sv=2018-03-  
28&sr=b&si=f563200f-b90d-45ff-b8ff-  
7970e301a718&sig=bpuyXzF5OyAWBcjzkLFMUZd%2BIEU3a0oOWS0Arq4tqoM%3D" --blob-  
type PageBlob
```

INFO: Scanning...

INFO: Any empty folders will not be processed, because source and/or destination doesn't have full folder support

Job aceff670-634d-7c41-47df-151b8e6d31a4 has started

Log file is located at: /Users/myUser/.azcopy/aceff670-634d-7c41-47df-151b8e6d31a4.log

Job aceff670-634d-7c41-47df-151b8e6d31a4 summary

Elapsed Time (Minutes): 2.7671

Number of File Transfers: 1

Number of Folder Property Transfers: 0

Total Number of Transfers: 1

Number of Transfers Completed: 1

Number of Transfers Failed: 0

Number of Transfers Skipped: 0

TotalBytesTransferred: 107377328640

Final Job Status: Completed

6. Once the VHD has been successfully uploaded, revoke the access. Use the following command:

```
az disk revoke-access -n <disk name> -g <resource group>
```

## Example

```
myUser@myUsermac:/Users/myUser/Desktop/MyCompany/AZURE_Cloud_Deployment/Fort  
iNAC  
> az disk revoke-access -n fortinac-9.2.1.0415_v4 -g MyResourceGroup
```

Proceed to [Create the Virtual Machine](#).

## Create the Virtual Machine

The steps in this section require the Azure CLI. The virtual machine can be created with or without a Public IP Address.

Proceed as appropriate:

[Option 1: Create Virtual Machine with Public IP Address](#)

[Option 2: Create Virtual Machine with Private IP Address only](#)

## Option 1: Public IP Address

1. Run the command

```
az vm create --resource-group <resource group> --location <Azure region> --name <disk name> --os-type linux --attach-os-disk <disk name>
```

### Example

```
myUser@myUser-  
mac:/Users/myUser/Desktop/MyCompany/AZURE_Cloud_Deployment/FortiNAC  
> az vm create --resource-group MyResourceGroup --location eastus --name  
fortinac-9.2.1.0415_v4 --os-type linux --attach-os-disk fortinac-  
9.2.1.0415_v4
```

It is recommended to use parameter "--public-ip-sku Standard" to create new VM with Standard public IP. Please note that the default public IP used for VM creation will be changed from Basic to Standard in the future.

```
{  
  "fqdns": "",  
  "id": "/subscriptions/3f4a7f4a-5e8a-408f-8b5b-c8bfeb836628/resourceGroups/MyResourceGroup/providers/Microsoft.Compute/virtualMachines/fortinac-9.2.1.0415_v4",  
  "location": "eastus",  
  "macAddress": "00-22-48-1D-B9-D9",  
  "powerState": "VM running",  
  "privateIpAddress": "10.32.0.6",  
  "publicIpAddress": "<public IP address>",  
  "resourceGroup": "MyResourceGroup",  
  "zones": ""  
}
```

2. **Important:** Edit the newly created VM to ensure it has sufficient RAM. Refer to the **Memory** column for the appropriate network size in the **VM Server Resource Sizing** table of the [FortiNAC Data Sheet](#). Refer to Microsoft documentation.

Related link

<https://docs.microsoft.com/en-us/azure/virtual-machines/sizes>

The Azure portal should now have a virtual machine named fortinac-9.2.1.0415\_v4 with a public IP address. This virtual machine should now be able to be accessed via SSH directly.

### Example

```
myUser@myUser-mac:/Users/myUser/Desktop/MyCompany/AZURE_Cloud_Deployment/FortiNAC
> ssh root@<public IP address>
```

```
*****
  Recognized platform: Linux
    Distribution: CentOS Linux release 7.9.2009 (Core)
      OS Kernel: 3.10.0-1160.36.2.el7.x86_64
    Home directory: /root
    Terminal type: xterm-256color

    Product Type: NetworkControlApplicationServer
    Appliance Type: FortiNAC FNUNL_
      Version: 9.2.1.0415 (GA)
    Build Date: Thu 04-Nov-2021
*****
```

Proceed to [Serial Console Configuration](#).



## Option 2: No Public IP Address

1. Run the command

```
az vm create --resource-group <resource group> --location <Azure region> --name <disk name> --os-type linux --attach-os-disk <disk name> --public-ip-address ""
```

### Example

```
myUser@myUser-mac:/Users/myUser/Desktop/MyCompany/AZURE_Cloud_Deployment/FortiNAC
> az vm create --resource-group MyResourceGroup --location eastus --name fortinac-9.2.1.0415_v4 --os-type linux --attach-os-disk fortinac-9.2.1.0415_v4 --public-ip-address ""
```

2. **Important:** Edit the newly created VM to ensure it has sufficient RAM. Refer to the **Memory** column for the appropriate network size in the **VM Server Resource Sizing** table of the [FortiNAC Data Sheet](#). Refer to Microsoft documentation.

### Related link

<https://docs.microsoft.com/en-us/azure/virtual-machines/sizes>

The Azure portal should now have a virtual machine named fortinac-9.2.1.0415\_v4 with a private IP address that can be accessed via SSH directly.

### Example

```
myUser@myUser-mac:/Users/myUser/Desktop/MyCompany/AZURE_Cloud_Deployment/FortiNAC
> ssh root@10.32.0.6
```

```
*****
Recognized platform: Linux
  Distribution: CentOS Linux release 7.9.2009 (Core)
    OS Kernel: 3.10.0-1160.36.2.el7.x86_64
  Home directory: /root
  Terminal type: xterm-256color

  Product Type: NetworkControlApplicationServer
  Appliance Type: FortiNAC FNUNL_
    Version: 9.2.1.0415 (GA)
    Build Date: Thu 04-Nov-2021
*****
```

Proceed to [Serial Console Configuration](#).

## Serial Console Configuration

1. Login to the Azure portal.  
<https://portal.azure.com/>
2. Navigate to **Virtual Machines**.
3. Select the FortiNAC VM.
4. Select **Boot Diagnostics > Setting**.
5. Enable with the Custom storage account created in section [Create Resource Group and Storage Account](#).
6. Save the settings.
7. Go to the Serial console and a CLI window should now appear. **Note:** May need to hit the “Enter” or “Return” key to get the window to update.

## Create Second Network Interface (eth1)

If the FortiNAC Service Network will be used to restrict network access for untrusted endpoints, create a second network interface. This interface represents eth1 or the FortiNAC Service Network interface. DNS and DHCP for restricted endpoints will be served from this interface.

1. Select **Networking > Virtual network/subnet > Subnets**.
2. Click **"+ Subnet"**.
3. Create the subnet to which the eth1 interface will be assigned.
4. Stop VM.
5. Click **Networking**
6. Click **Attach Network Interface**
7. Click **Create and Attach Network Interface**
8. Configure the interface:
  - Network Interface Name: NAC Service Network
  - Select the new subnet from drill down
  - NIC network security group: Basic (?)
  - Private IP address assignment: Static
  - Enter IP address
9. Click **Create**
10. Start VM
11. Reconnect via SSH to the FortiNAC VM using the static address configured within the default route (not eth1).
12. Verify both eth0 and eth1 are created by typing **ifconfig**

### Related Links

Configuring multiple network interfaces:

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/multiple-nics?toc=/azure/virtual-network/toc.json>

Adding and removing network interfaces:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-vm>

## Add Security Rules

Security rules are needed to connect to the UI and allow traffic from the restricted networks.

1. Navigate to the **Azure Portal > Virtual Machines**. Select the FortiNAC VM instance.
2. Select **Networking**.
3. Add inbound rules to allow TCP access to the UI.

## Configure Subnets Security Rules and Route Tables for eth1 Access

On the interface created to represent eth1:

- Create subnets for each network that will be used (production & restricted)
- Create Security Rules to allow traffic for each of the subnets specified. For a list of required ports, refer to the **Open Ports** section of the [Deployment Guide](#).
- Create a Route Table on the interface
  - Name:
  - Address Prefix: <network for DHCP scope>/<mask>
  - Next hop type: Virtual appliance
  - Next hop IP address: <gateway ip>

## Assign a Static IP Address

1. SSH to the FortiNAC VM. Login to the FortiNAC CLI using the following:  
User name = admin  
Password = admin
2. Use the command `route -n` to get the default route. Exit by typing `logout`.
3. Navigate to the **Azure Portal > Virtual Machines**. Select your FortiNAC VM instance.
4. Select **Networking > Network Interface > IP configurations**.
5. Select the primary interface.
6. Set the Private IP address settings to Static and assign a private address that is within the subnet of the default route.

Appliance installation is complete. Proceed to the [FortiNAC Deployment Guide](#) to continue deployment.

# Appendix

## Install the Azure CLI

Refer to the following link for installing Azure CLI and working with azcopy:

<https://docs.microsoft.com/en-us/cli/azure/install-azure-cli>

For Reference:

```
myUser@myUser-mac:/Users/myUser
> az version
{
  "azure-cli": "2.29.1",
  "azure-cli-core": "2.29.1",
  "azure-cli-telemetry": "1.0.6",
  "extensions": {}
}
```

```
myUser@myUser-mac:/Users/myUser
> azcopy -v
azcopy version 10.13.0
```

## Related Links

**Configuring multiple network interfaces:**

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/multiple-nics?toc=/azure/virtual-network/toc.json>

**Adding and removing network interfaces:**

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-vm>

### **AZURE Secure and Private Topology with FortiNAC**

**Site to Site VPN Gateways**

<https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal>

**Creating a Virtual Network with using a FortiGate➔Azure IPSEC connection**

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/255100/ipsec-vpn-to-azure>



**FORTINET®**



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.