Deployment Guide
Sep-2017 rev. a

FortiGate VM Deployment Guide for AVX Series Network Functions Platform

Table of Contents

1. About FortiGate VM on AVX

Array Networks AVX Series network functions platforms offer a multi-tenant virtualized platform that supports deployment of multiple Virtual Appliance (VA) instances or Virtual Network Functions (VNFs) with guaranteed performance, which enables organizations to consolidate their data centers without sacrificing performance, stability and flexibility.

FortiGate Virtual Machines (VMs) allow you to mitigate blind spots by implementing critical security controls within your virtual infrastructure. They also allow you to rapidly provision security infrastructure whenever and wherever it is needed. FortiGate VMs feature all of the security and networking services common to traditional hardware-based FortiGate appliances.

Fortinet provides a virtual version of FortiGate, which is suitable for deploying on the AVX appliance. The FortiGate VM will be deployed on the AVX appliance as a VA instance. The FortiGate VM supports the entry, small, medium and large instance sizes provided by the AVX appliance. The FortiGate VM on AVX provides the following benefits:

- AVX provides guaranteed performance for the FortiGate VM, in contrast to other common hypervisors.
- AVX provides high scalability for the FortiGate VM and allows a pay-as-you-grow license model.
- FortiGate VMs and Array and other 3rd party networking and security products can be deployed as a service chain on an AVX.

Note: For this deployment guide, the AVX Series should run ArrayOS AVX 2.4.0.3 or later, and the FortiGate VM should run FortiOS 5.4 version or later.

For additional information about FortiGate, please visit https://www.fortinet.com.

2. Deploying the FortiGate VM on AVX

To deploy a FortiGate VM on the AVX appliance, follow these steps:

1. Obtain the image of the FortiGate VM
2. Import the image to the AVX appliance
3. Create a VA Instance with the image on the AVX appliance
4. Assign virtual traffic ports to the VA instance
5. Start the VA Instance

2.1. Obtaining the Image of the FortiGate VM

Before deploying a FortiGate VM, contact Array Networks to obtain the image (for example, fortigate.qcow2) of the FortiGate VM as well as the metadata file (metadata.ini) of the image.

Please place the image and the metadata file onto an HTTP server or FTP server that is accessible by the AVX appliance. For example, the URLs of the image and the metadata file are http://10.4.0.35/fortigate.qcow2 and http://10.4.0.35/metadata.ini respectively.

2.2. Importing the Image to the AVX Appliance

To import the image to AVX, execute the following command on AVX:

va image <*image_name*> <*url*> *[format] [metadata_url]*

image_name: the name of the image.

url: the URL of the image.

format: the format of the image: qcow2, raw, vmdk or tgz.

metadata_url: the URL of the image's metadata file.

```
AN(config)#va image FortiGate-image http://10.4.0.35/fortigate.qcow2 qcow2
http://10.4.0.35/metadata.ini
```

2.3. Creating the FortiGate VM with the Image on the AVX Appliance

After the image has been imported successfully, you can create the VA instance using the following command:

va pureinstance <*va_name*> <*va_size*> *[domain_id] [image_name]*

va_name: name of the VA instance.

va_size: size of the VA instance.

domain_id: ID of the NUMA domain from which system resources are assigned.

image_name: name of the image.

```
AN(config)#va pureinstance FortiGate-VM medium 1 FortiGate-image
```

The size of the VA instance determines the amount of system resources assigned to the VA instance.

Size	CPU	Memory
Entry	1 core	2GB
Small	2 cores	4GB
Medium	4 cores	8GB
Large	8 cores	16GB

2.4. Assign Virtual Traffic Ports to the FortiGate VM

The AVX assigns a virtual management port that is connected with the AVX's physical management port using a built-in virtual switch when a FortiGate VM is created. The virtual management port becomes the first port (port1) for the FortiGate VM. It is recommended that the virtual management port be used for management purposes only.

To process data traffic, you will need to assign virtual traffic ports to the FortiGate VM according to the requirements of different deployment modes, as shown in the table below.

The AVX appliance provides two types of virtual traffic ports for the FortiGate VM:

- SR-IOV virtual ports: SR-IOV Virtual Function (VF) of a 10G traffic port.
- Virtio virtual ports: virtio-type ports assigned by the virtual switch to the attached VA instance.

Deployment Mode	Requirements
NAT/Route mode	Assign one or more SR-IOV virtual ports
Transparent mode	Assign one or multiple pairs of virtio virtual ports

2.4.1. Assigning an SR-IOV Virtual Port to the FortiGate VM

With SR-IOV, one physical traffic port on the AVX can be virtualized as eight SR-IOV virtual ports.

To assign an SR-IOV virtual port, execute the following command:

va port <*va_name*> <*port_name*> <*vf_index*>

va_name: name of the VA instance.

port_name: name of the physical traffic port.

vf_index: Index of the SR-IOV VF to be assigned. The indexes of eight SR-IOV virtual ports under one physical traffic port are 1 to 8 respectively.

```
AN(config)#va port FortiGate-VM port1 1
```

2.4.2. Assigning a Virtio Virtual Port to the FortiGate VM

When you attach the FortiGate VM to a virtual switch, the FortiGate VM will be assigned a virtio virtual port. For external communication of the FortiGate VM using a virtio virtual port, you also need to add a physical traffic port to the virtual switch. In this way, the virtio virtual port can send traffic to the network via the physical traffic port.

To create a virtual switch, execute the following command:

switch name <*virtual_switch_name*>

virtual_switch_name: name of the virtual switch

```
AN(config)#switch name switch1
```

To attach the FortiGate VM to the virtual switch, execute the following command:

switch va <*virtual_switch_name*> <*va_name*> <*vport_name*> *[vlan_tag] [queue_number]*

virtual_switch_name: name of the virtual switch

va_name: name of the VA instance

vport_name: name of the virtual switch

vlan_tag: tag of the VLAN to which the virtio virtual port belongs.

queue_number: number of Rx/Tx queue pairs enabled for the virtio virtual port.

```
AN(config)#switch va switch1 FortiGate-VM vport1 0 4
```

Note: The AVX provides multi-queue support to maximize the network performance of the virtio virtual port as the number of vCPUs increases. Please enable a specified number of Rx/Tx queue pairs in the “queue_number” parameter according to the number of vCPUs assigned to the VA instance. For example, enable four queue pairs for a medium-size VA instance.

To add a traffic port to the virtual switch, execute the following command:

switch interface <*virtual_switch_name*> <*interface_name*>

virtual_switch_name: name of the virtual switch

interface_name: name of the physical traffic port.

```
AN(config)#switch interface switch1 port1
```

Note: For the FortiGate VM to support the transparent deployment mode, you need to create two virtual switches, attach the FortiGate VM to both of them, and add two traffic ports to the two virtual switches respectively.

2.5. Starting the FortiGate VM

After the FortiGate VM is created, you can start it using the “**va start** <*va_name*>” command.

```
AN(config)#va start FortiGate-VM
```

3. Completing Initial Configuration for the FortiGate VM

After the FortiGate VM is up, you can establish a console connection to it using the "**va console** <*va_name* >" command.

```
AN(config)#va console FortiGate-VM
```

Before you can connect to the FortiGate VM Web-based manager you must configure a network interface on the console connection. Once an interface with administrative access is configured, you can connect to the FortiGate VM Web-based Manager and start advanced configurations.

To complete the initial configuration, follow these steps:

1. Log into the console with the username "admin". By default there is no password. Just press **Enter**.
2. Configure the IP address for the management interface (port1).

```
config system interface
edit port1
set ip 192.168.0.100 255.255.255.0
set allowaccess ping https ssh http fgfm
end
```

Note: The ping, https, ssh, and fgfm protocols are enabled on the port1 interface by default.

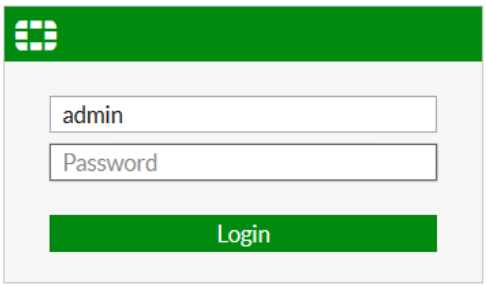
3. Configure the default gateway.

```
config router static
edit 1
set device port1
set gateway 192.168.0.1
end
```

4. Configure DNS.

```
config system dns
set primary 192.168.0.1
set secondary 192.168.0.10
end
```

When the initial configuration is completed, you can access the FortiGate VM Web-based Manager at https://<management_IP>, from which you can proceed with the configuration. The default username is "admin" and the default password is empty.



Note: Remember to change the default password after you log in to the WebUI.

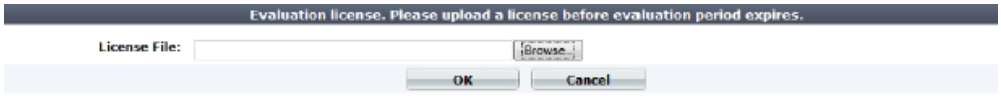
For more information, please refer to the online help of the FortiGate product (http://docs.fortinet.com/fortigate/admin-guides).

4. Loading a Formal License to the FortiGate VM

To make full use of functionality and performance of the FortiGate VM, you need to purchase and upload a valid formal license.

To upload a valid formal license, follow these steps:

1. Contact Array Networks Customer Support to purchase a formal license by providing the size of the VA instance. Store the license on a device that is accessible to the AVX.
2. Access the Web-based Manager and go to **System > Dashboard > Status**. In the **License Information** widget, click the **Update** button.
3. In the prompted window, click the **Browse** button to locate the license file and click **OK**.



After a license is uploaded, the FortiGate VM will communicate with the FortiGuard Distribution Network (FDN) for license validation. The VM registration status appears as valid in the **License Information** widget after the license has been validated.

5. Deployment Examples

5.1. Supported Operating Modes

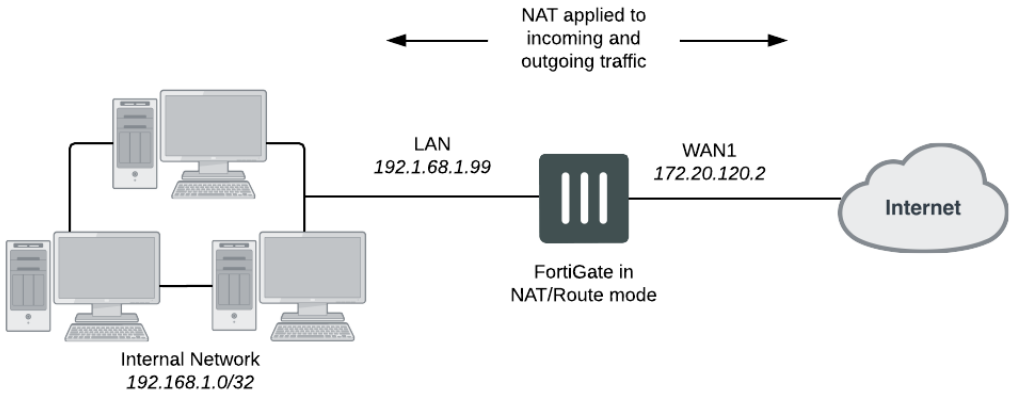
The FortiGate VM on AVX can support the same deployment modes as its hardware counterpart:

- NAT/Route
- Transparent

5.1.1. NAT/Route Mode

The most common of the two operating modes is NAT/Route mode, where a FortiGate is installed as a gateway or router between two networks. In most cases, it is used between a private network and the Internet. This allows the FortiGate to mask the IP addresses of the private network using Network Address Translation (NAT).

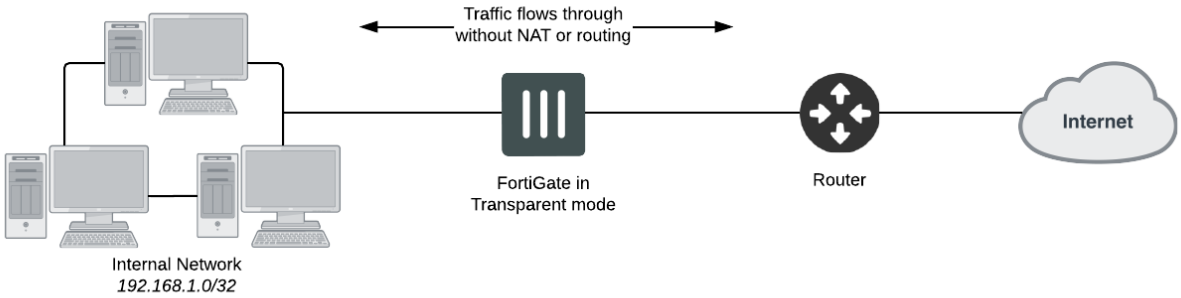
The following figure displays the deployment of the FortiGate VM in NAT/Route mode.



5.1.2. Transparent Mode

A FortiGate in Transparent mode is installed between the internal network and the router. In this mode, the FortiGate does not make any changes to IP addresses and only applies security scanning to traffic. When a FortiGate is added to a network in Transparent mode, no network changes are required, except to provide the FortiGate with a management IP address. Transparent mode is used primarily when there is a need to increase network protection but changing the configuration of the network itself is impractical.

The following figure displays the deployment of the FortiGate VM in Transparent mode.

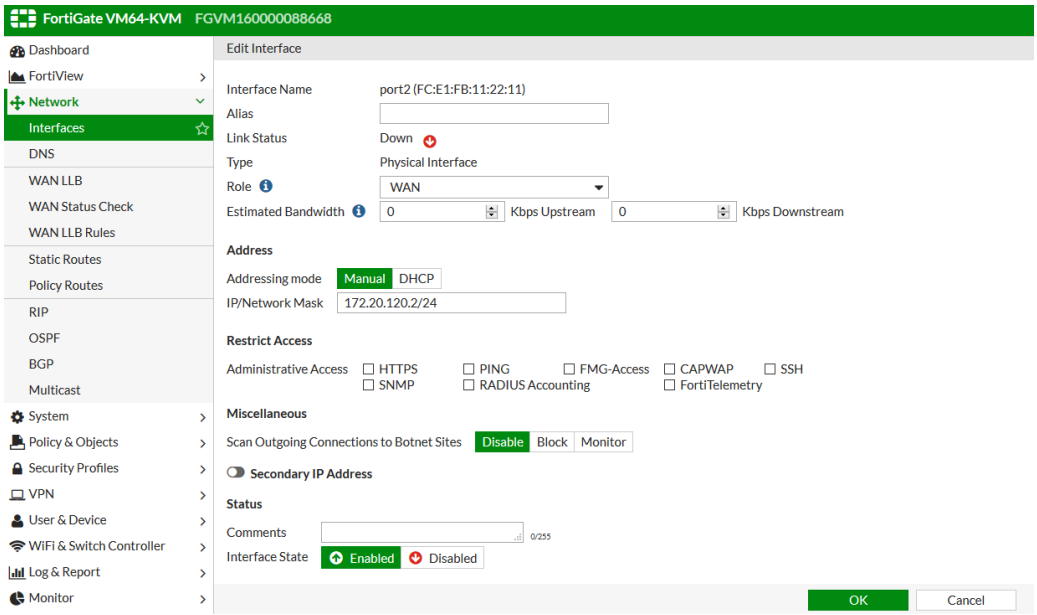


5.2. Configuration Example

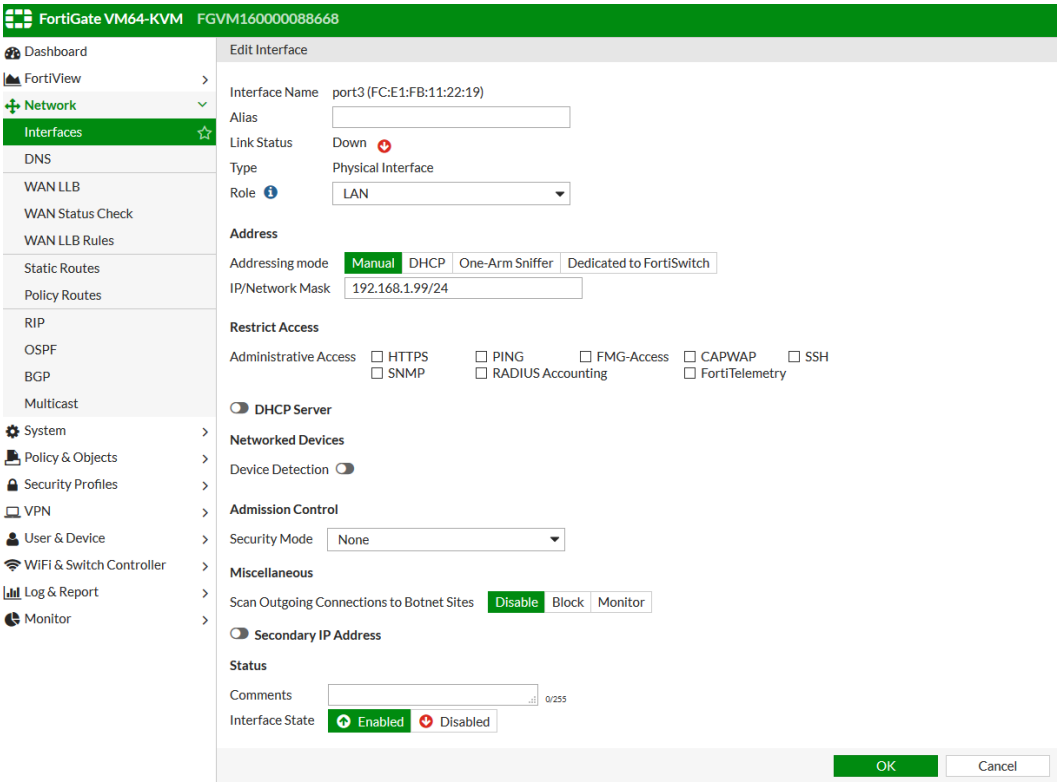
5.2.1. Configuring the NAT/Route Mode

To configure the NAT/Route mode, follow these steps:

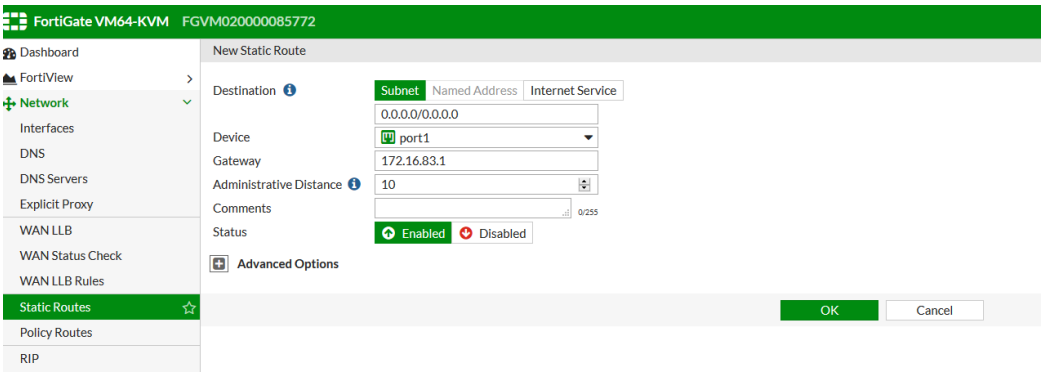
1. Access the WebUI of the FortiGate VM (for example, https://192.168.1.100:443).
2. Go to **Network > Interfaces** and edit the Internet-facing interface. Set **Role** to **WAN**, **Addressing Mode** to **Manual** and **IP/Netmask** to your public IP address. Select **OK**.



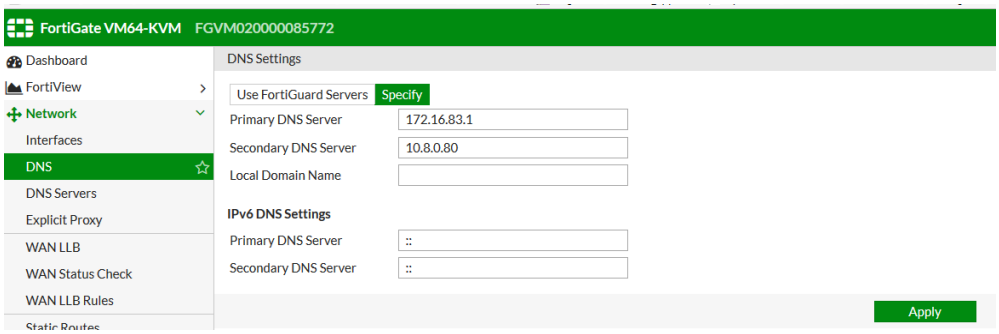
3. Edit the interface connecting the internal network. Set **Role** to **LAN**, **Addressing Mode** to **Manual** and **IP/Netmask** to your private IP address. Select **OK**.



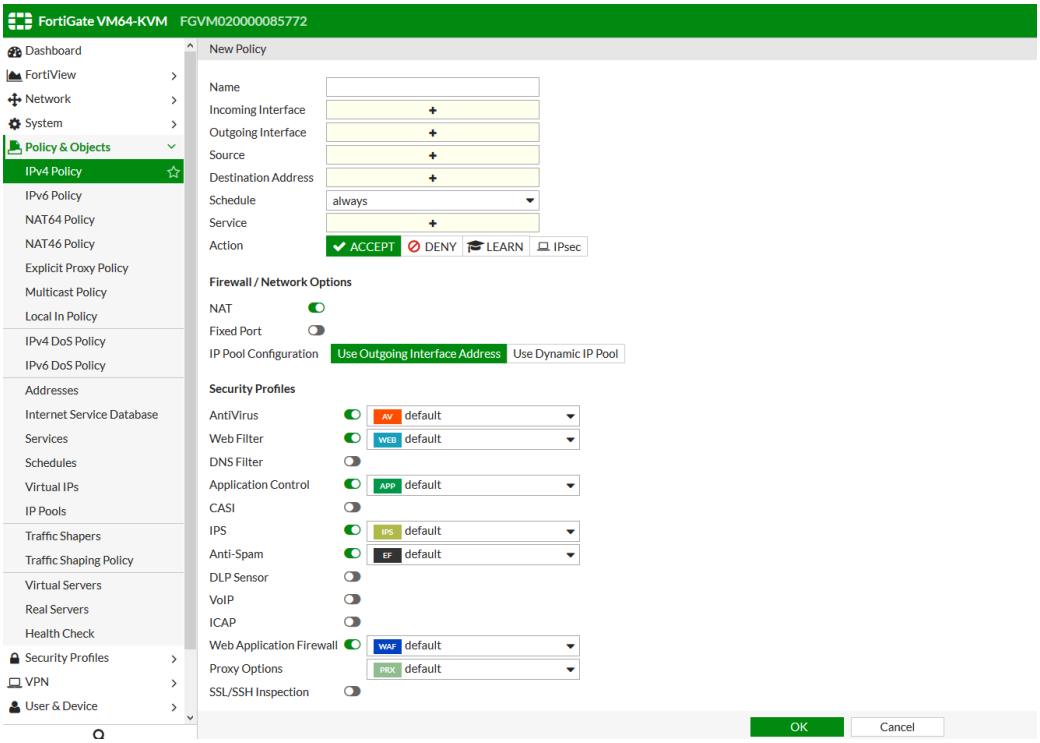
4. Go to **Network > Static Routes** and select **Create New** to add a default route. Set **Destination** to **Subnet** (which allows you to input a numeric IP address or subnet), **Destination IP/Mask** to 0.0.0.0/0.0.0.0, **Device** to the Internet-facing interface, and **Gateway** to the gateway (or default route) provided by your ISP or to the next hop router, depending on your network requirements. Select **OK**.



5. (Optional) The FortiGate's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **Network > DNS**, select **Specify**, and add **Primary** and **Secondary** DNS servers. Select **Apply**.



6. Go to **Policy & Objects > IPv4 Policy** and select **Create New** to add a security policy that allows users on the private network to access the Internet. In the policy, set the **Incoming Interface** to the interface connecting the internal network and the **Outgoing Interface** to the Internet-facing interface. You will also need to set **Source**, **Destination Address**, **Schedule**, and **Service** according to your network requirements. You can set these fields to the default all/ANY settings for now but should create the appropriate objects later after the policies have been verified. Make sure the **Action** is set to **ACCEPT**. Turn on **NAT** and make sure **Use Outgoing Interface Address** is selected. Select **OK**.



Note: If your network uses IPv6 addresses, go to **Policy & Objects** > **IPv6 Policy** and select **Create New** to add a security policy that allows users on the private network to access the Internet. If the IPv6 menu option is not available, go to **System > Feature Select**, turn on **IPv6**, and select **Apply**.

The NAT/Route mode is now configured.

5.2.2. Configuring the Transparent Mode

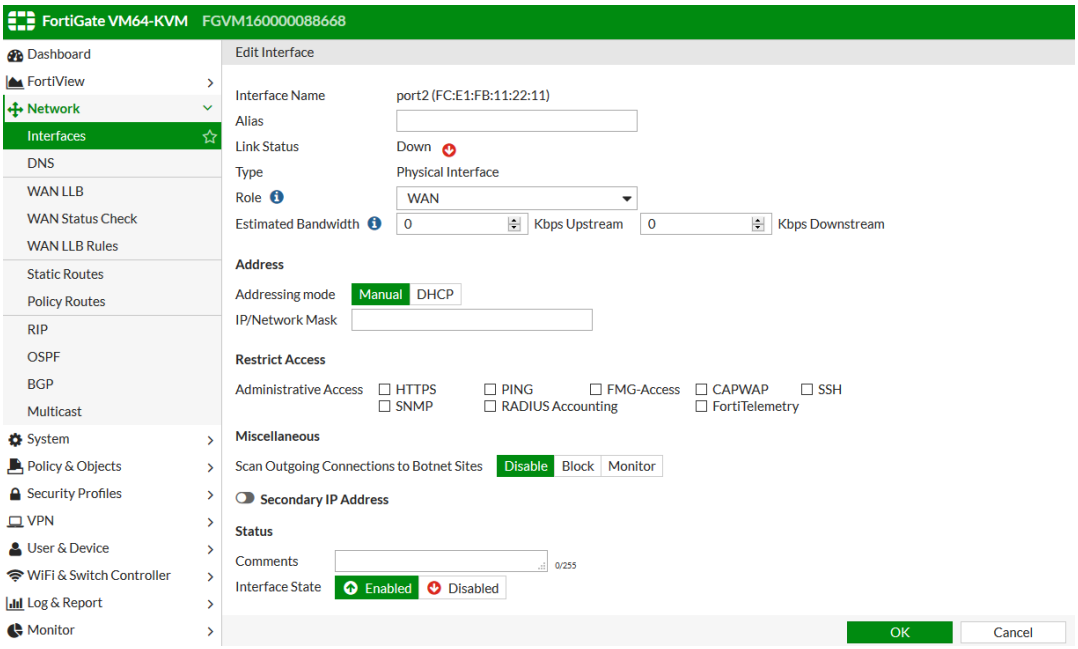
To configure the Transparent mode, follow these steps:

1. Before connecting the FortiGate VM to your network, enter the following command into the CLI Console to change the operation mode to Transparent, and set the management IP address and the default route.

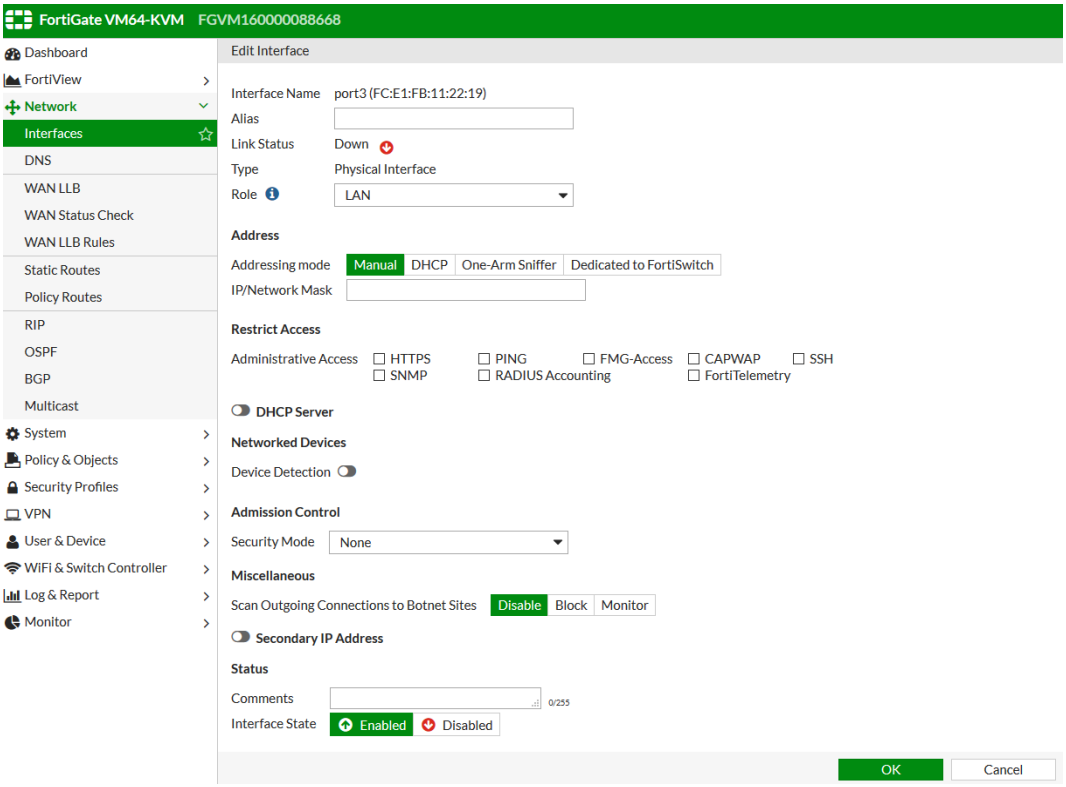
```
config system settings
set opmode transparent
set manageip <address and netmask>
set gateway <address>
end
```

2. Access the WebUI of the FortiGate VM (for example, https://192.168.1.100:8443).

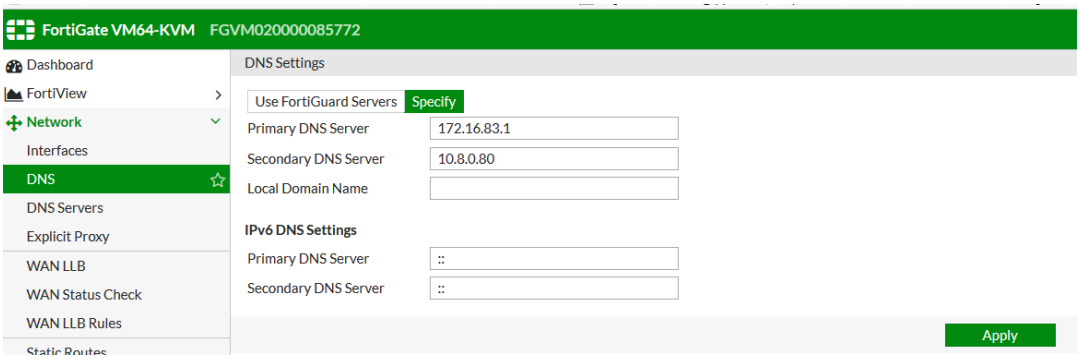
3. Go to **Network > Interfaces** and edit the Internet-facing interface. Set **Role** to **WAN** and select **OK**.



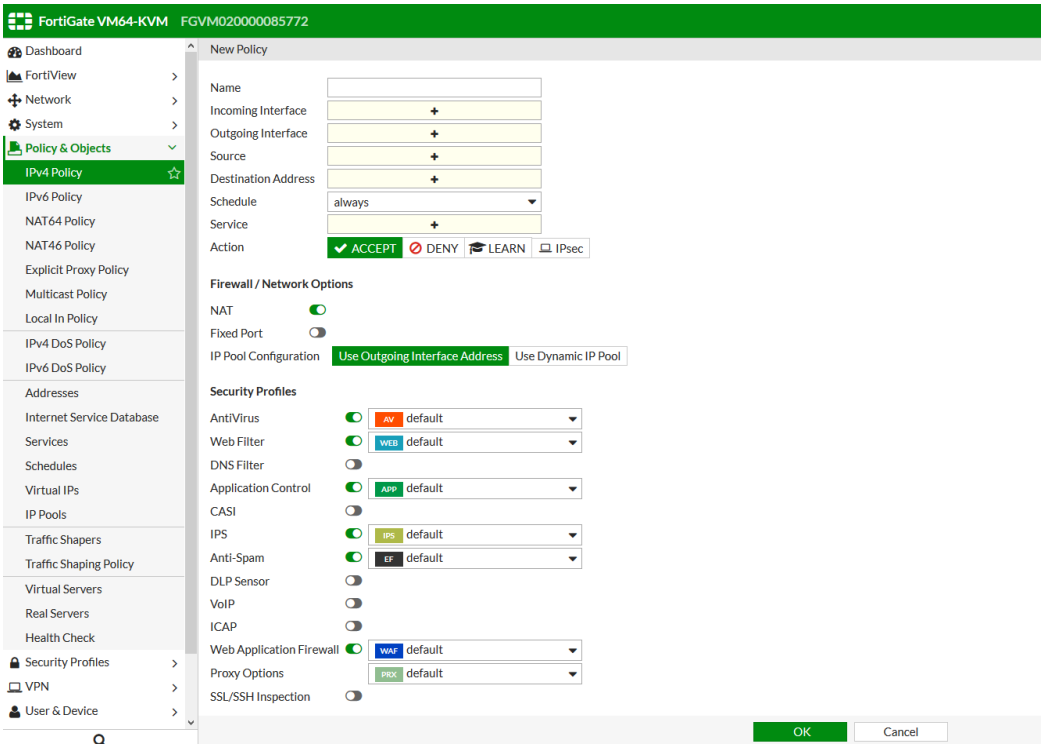
4. Edit the interface connecting the internal network. Set **Role** to **LAN** and select **OK**.



5. (Optional) The FortiGate's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **Network > DNS**, select **Specify**, and add **Primary** and **Secondary** DNS servers. Select **Apply**.



6. Go to **Policy & Objects > IPv4 Policy** and select **Create New** to add a security policy that allows users on the private network to access the Internet. In the policy, set the **Incoming Interface** to the interface connecting the internal network and the **Outgoing Interface** to the Internet-facing interface. You will also need to set **Source**, **Destination Address**, **Schedule**, and **Service** according to your network requirements. You can set these fields to the default all/ANY settings for now but should create the appropriate objects later after the policies have been verified. Make sure the **Action** is set to **ACCEPT**. Select **OK**.



Note:

- If your network uses IPv6 addresses, go to **Policy & Objects** > **IPv6 Policy** and select **Create New** to add a security policy that allows users on the private network to access the Internet. If the IPv6 menu option is not available, go to **System > Feature Select**, turn on **IPv6**, and select **Apply**.
- It is recommended to avoid using any security profiles, such as antivirus or web filtering, until after you have successfully installed the FortiGate VM. After the installation is verified, you can apply any required security profiles.

The Transparent mode is now configured.

About Array Networks

Array Networks, the network functions platform company, develops purpose-built systems for deploying virtual app delivery, networking and security functions with guaranteed performance. Headquartered in Silicon Valley, Array is backed by over 250 worldwide employees and is poised to capitalize on explosive growth in the areas of virtualization, cloud and software-centric computing. Proven at over 5000 worldwide customer deployments, Array is recognized by leading analysts, enterprises and service providers, for next-generation technology that delivers agility at scale.

Corporate Headquarters
info@arraynetworks.com
408-240-8700
1 866 MY-ARRAY
www.arraynetworks.com

EMEA
rschmit@arraynetworks.com
+32 2 6336382

China
support@arraynetworks.com.cn
+010-84446688

France and North Africa
infosfrance@arraynetworks.com
+33 6 07 511 868

India
isales@arraynetworks.com
+91-080-41329296

Japan
sales-japan@
arraynetworks.com
+81-44-589-8315

To purchase Array Networks Solutions, please contact your Array Networks representative at 1-866-MY-ARRAY (692-7729) or authorized reseller

May-2017 rev. a