

# **FortiGate-VM HA Deployment Guide for AVX Series Network Functions Platform**

# Table of Contents

<b>Table of Contents .....</b>	<b>1</b>
<b>1. Introduction.....</b>	<b>2</b>
<b>2. Prerequisites.....</b>	<b>3</b>
2.1. Array Networks AVX Network Functions Platform .....	3
2.2. Fortinet FortiGate-VM Instances .....	3
<b>3. Network Topology .....</b>	<b>4</b>
<b>4. Configuring AVX1 .....</b>	<b>5</b>
<b>5. Deploying the FortiGate-VM instance on AVX1 .....</b>	<b>6</b>
5.1. Obtain the Image of the FortiGate-VM .....	6
5.2. Import the Image to the AVX Appliance .....	6
5.3. Create a VA instance with the Image on the AVX Appliance .....	6
5.4. Assign Virtual Traffic Ports to the VA Instance .....	7
5.5. Start the VA Instance .....	8
<b>6. Configuring the FortiGate-VM Instance on AVX1 .....</b>	<b>9</b>
<b>7. Configuring AVX2.....</b>	<b>12</b>
<b>8. Deploying the FortiGate-VM Instance on AVX2 .....</b>	<b>13</b>
<b>9. Configuring the FortiGate-VM Instance on AVX2 .....</b>	<b>14</b>
<b>10. Verifying the FortiGate-VM HA on AVX Configuration .....</b>	<b>16</b>

# 1. Introduction

Array Networks AVX Series network functions platforms host multiple Array and 3rd-party virtual appliances, providing the agility of cloud and virtualization with the guaranteed performance of dedicated appliances.

Array's AVX Series network functions platform hosts up to 32 fully independent virtual appliances (VAs), including Array load balancing, SSL VPN and WAF as well as 3rd-party VAs from leading networking and security vendors. Designed with managed service provider and enterprises in mind, the AVX Series enables data center consolidation without sacrificing the agility of cloud and virtualization or the performance of dedicated appliances. Uniquely capable of assigning dedicated CPU, SSL, memory and interface resources per VA, the AVX Series network functions platform is the only solution to deliver guaranteed performance in shared environments.

A firewall is a network security device that monitors incoming and outgoing network traffic and determines whether to allow or block specific traffic based on a defined set of security rules. A firewall sandwich is a deployment in which multiple firewalls are sandwiched between a pair of load balancers to improve availability, scalability, and manageability across the IT infrastructure.

The following sections will describe the steps required to deploy a Fortinet FortiGate-VM HA (High Availability) on the AVX Series network functions platform.

The Fortinet FortiGate-VM (Virtual Machine) is a Next-Generation Firewall that offers flexible deployments from the network edge to the core, data center, internal segment, and the cloud. FortiGate-VM firewalls delivers scalable performance of advanced security services like threat protection, SSL inspection, and ultra-low latency for protecting internal segments and mission critical environments. For the purposes of this deployment guide, the FortiGate-VM will be deployed on the AVX as a VA instance.

## 2. Prerequisites

This deployment guide requires the following hardware and software products.

### 2.1. Array Networks AVX Network Functions Platform

- Two AVX Series (x600 or x800 models) network functions platform running version ArrayOS 2.7.0.34 or later

The AVX appliance can be purchased from Array Networks or authorized resellers. For more information on deploying the AVX appliance, please refer to the AVX Web UI Guide, which is accessible through the product's Web User Interface.

### 2.2. Fortinet FortiGate-VM Instances

- Two FortiGate-VM (VM02, VM04 or VM08) instances running version 6.0.2 or later for the KVM hypervisor. One FortiGate-VM instance will be deployed on each AVX platform. Ensure the AVX platforms have enough hardware resources to support the FortiGate-VM instances.

The FortiGate-VM instances may be purchased from Fortinet or a reseller. For more information on deploying the FortiGate-VM instances for KVM, please visit <https://www.fortinet.com>.

**Note:** Assuming you have all these components, it should roughly take **90-120** minutes to complete the entire configuration in this deployment guide.

### 3. Network Topology

Figure 1 shows a detailed configuration of the FortiGate-VM HA on AVX deployment.

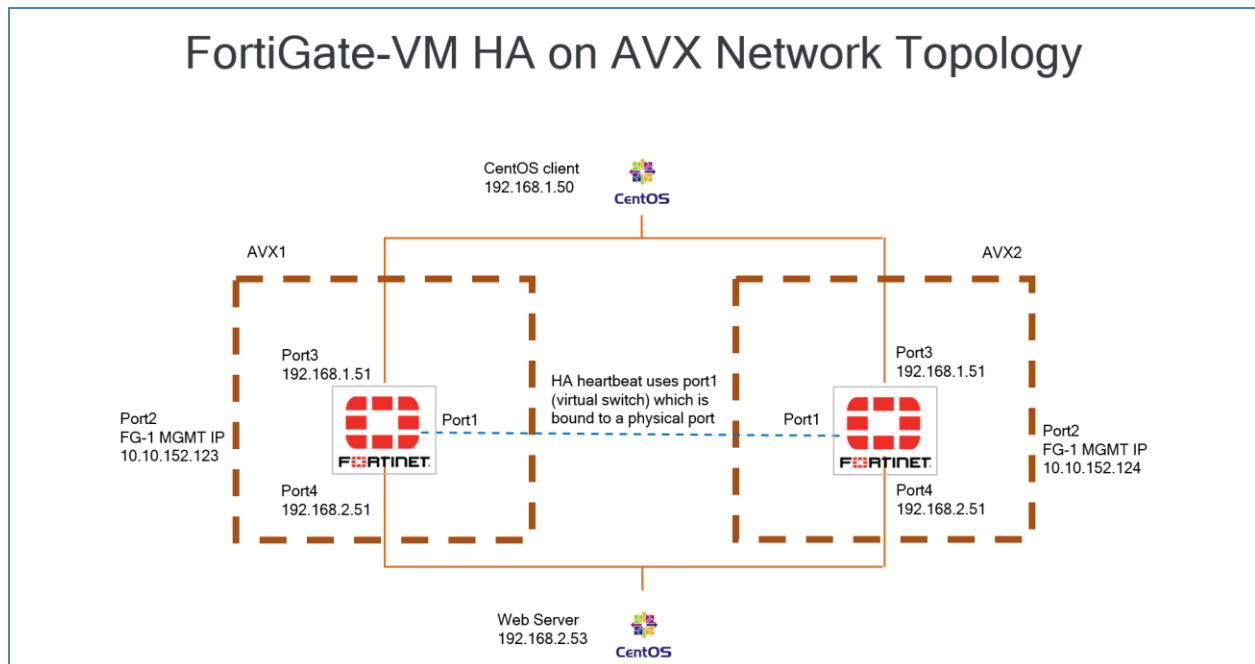


Figure 1 – Deployment Details

In this deployment, there is one FortiGate-VM instance running on each of the AVX platforms. The FortiGate-VM instances will have identical IP configuration on the ingress (port3) and egress (port4) interfaces. Port3 and port4 are the traffic ports and both use the SR-IOV ports. The HA heartbeat uses port1. Port1 is a virtual port on the virtual switch. The virtual switch is bound to an SR-IOV port for external communication.

#### Typical Traffic Flow: Inbound

The client machine is running CentOS and the Web Server is running CentOS, both external to the AVX platforms. The two CentOS machines are required only to validate the design.

The client (top) will generate Web Server (bottom) requests to the CentOS Web Servers via the FortiGate-VM instance. In the event of HA failure and the master/active FortiGate-VM instance fails, the standby FortiGate-VM instance will take over as the master/active FortiGate-VM. If the original master/active FortiGate-VM instance becomes active again, it will resume ownership as the master/active instance.

## 4. Configuring AVX1

To configure the first AVX appliance, follow these steps:

1. Login to the AVX console using default credentials.

```
Login: array
```

```
Password: admin
```

2. Type “enable” and hit the <Enter> key twice to enter enable mode. No password is required.

```
AN>enable
```

```
Enable password:
```

```
AN#
```

3. Type “config terminal” to enter config mode.

```
AN#config terminal
```

```
AN(config)#
```

4. Change the hostname to AVX1.

```
AN(config)#hostname AVX1
```

```
AVX1(config)#
```

5. Configure the IP address and default gateway for the management port.

```
AVX1(config)#ip address 10.10.152.171 255.255.255.0 (use your own IP)
```

```
AVX1(config)#ip route default 10.10.152.1 (use your own gateway IP)
```

6. Enable WebUI.

```
AVX1(config)#webui on
```

7. Save changes.

```
AVX1(config)#write memory
```

You may now access the AVX1 appliance using the WebUI at <https://<IP>:8888>. In this example, <https://10.10.152.171:8888>.

## 5. Deploying the FortiGate-VM instance on AVX1

To deploy the FortiGate-VM instance 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

Licenses are required for each VA instance. Please contact Fortinet to obtain licenses.

### 5.1. Obtain the Image of the FortiGate-VM

Before deploying a FortiGate-VM, please contact Fortinet to obtain the KVM image. KVM images can be directly uploaded to the AVX. Please consult the AVX Application Guide or AVX CLI Handbook for additional instructions on how to upload and create a VA instance.

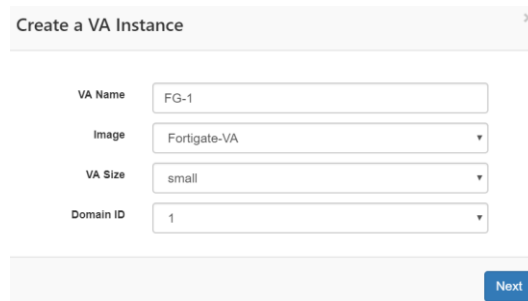
### 5.2. Import the Image to the AVX Appliance

On the AVX WebUI, navigate to **VA Management > VA Image** to upload the FortiGate-VM image.

### 5.3. Create a VA instance with the Image on the AVX Appliance

On the AVX WebUI, navigate to **VA Management > VA** to create the VA instance using the FortiGate-VM image.

1. Create a FortiGate-VM VA instance named FG-1. Select the VA size to match the FortiGate-VM instance size you are installing (see table below).



Create a VA Instance

VA Name:

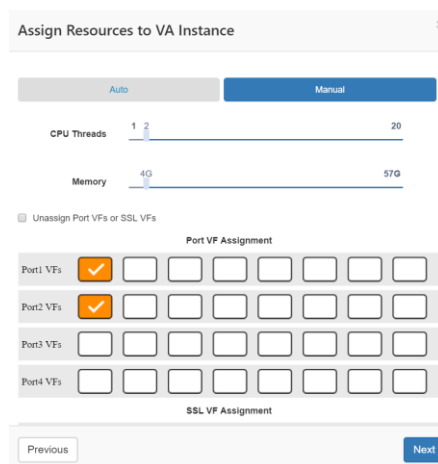
Image:

VA Size:

Domain ID:

FortiGate VM Version	Recommended AVX Instance Size
FortiGate VM02	Small (2 vCPUs, 4G RAM/Instance)
FortiGate VM04	Medium (4 vCPUs, 8G RAM/Instance)
FortiGate VM08	Large (8 vCPUs, 16G RAM/Instance)

2. Configure two traffic ports using the SR-IOV ports. Select the **Manual** option.



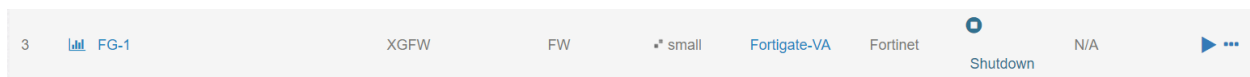
The dialog box titled "Assign Resources to VA Instance" has a close button (X) in the top right. It features two tabs: "Auto" and "Manual", with "Manual" selected. Below the tabs are two sliders: "CPU Threads" ranging from 1 to 20, and "Memory" ranging from 4G to 57G. A checkbox labeled "Unassign Port VFs or SSL VFs" is present. Below this is a section for "Port VF Assignment" with a grid of checkboxes for Port1 VFs through Port4 VFs, each with 8 columns. Port1 and Port2 have their first checkboxes checked. Below the grid is an "SSL VF Assignment" section. At the bottom are "Previous" and "Next" buttons.

3. Confirm the VA Instance Configuration.



The dialog box titled "Confirm VA Instance Configuration" has a close button (X) in the top right. It displays a list of configuration parameters and their values: VA Name (FG-1), VA Size (small), Domain (1), Image (Fortigate-VA), CPU Threads (2), Memory (4G), Traffic Interface VFs (port1\_1, port2\_1), and SSL VFs (N/A). At the bottom are "Previous" and "Save" buttons.

4. Click on **Save**. Navigate to **VA Management > VA** to view your newly created VA instance

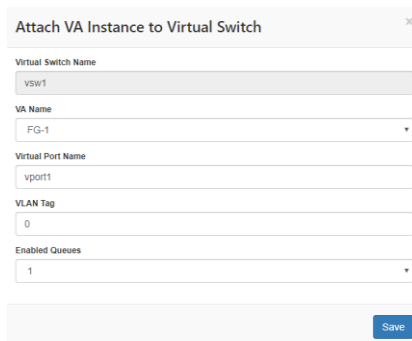


3	FG-1	XGFW	FW	* small	Fortigate-VA	Fortinet	Shutdown	N/A	▶ ...
---	------	------	----	---------	--------------	----------	----------	-----	-------

## 5.4. Assign Virtual Traffic Ports to the VA Instance

In this deployment, the AVX platform's built-in virtual switch will be used for the High Availability (HA) heartbeat. The virtual switch will be bound to an SR-IOV port to interconnect to the other AVX. On the AVX WebUI, navigate to **Platform > Network > Virtual Switch** to create virtual switches.

1. Create a Virtual Switch named vsw1 and attach the FG-1 VA instance. Assign the Virtual Port Name to vport1.



The dialog box titled "Attach VA Instance to Virtual Switch" has a close button (X) in the top right. It contains several input fields: "Virtual Switch Name" (vsw1), "VA Name" (FG-1), "Virtual Port Name" (vport1), "VLAN Tag" (0), and "Enabled Queues" (1). A "Save" button is at the bottom right.



2. Click on **Save**.

#	Virtual Switch Name	VA Name	Virtual Port Name	VLAN Tag	Enabled Queues	Action
1	vsw1	FG-1	vport1	0	1	<a href="#">+</a> <a href="#">-</a>

3. Click on the **General Settings** tab and toggle the **Binding Interface**. Select an available SR-IOV port for binding. In our example, port3 is selected.

Virtual Switch / vsw1

General Settings | Attaching VA Instances | Port Mirroring

STP: ☐ Disable

STP Priority:

Binding Interface:

4. Click Apply Changes.
5. Confirm the interfaces are correct for FG-1 by navigating to **VA Management > VA** and selecting FG-1.

VA Instance List / FG-1

Overview

Note: VA instance (FG-1) is not running. Please start it first.

Network Throughput (Mbps):

CPU Usage (%):

Memory Usage (%):

Disk Usage (%):

Management IP: Not configured

Assigned Platform Resources:

- CPU Threads: 2
- RAM: 4 GB
- Traffic Interface VFs: port2-1, port1-1
- Virtual Ports: vport1
- Passthrough Ports: Not bound
- SSL VFs: Not bound

Port Sequence:

#	Assigned AVX Port Resource	MAC	VA Port ID	VLAN Tag
1	mgmt	fc:a1:8b:9f:1b:13	1	/
2	port1.1	fc:a1:8b:9c:1a:00	1	/
3	port2.1	fc:a1:8b:9c:1a:00	1	/
4	vsw1 vport1	fc:a1:8b:9f:1b:10	1	0

You should see one management port, two SR-IOV traffic ports and a virtual port.

## 5.5. Start the VA Instance

On the AVX WebUI, navigate to **VA Management > VA** to start the VA instance.

1. Locate the VA instance named FG-1 and click on the ► symbol under the Action column to start the VA instance.

#	VA Name	VA Type	VA Size	VA Status	VA Last Update
3	FG-1	XGFW	FW	small	Fortigate-VA

Fortinet Running 2019-05-06T17:20:16

## 6. Configuring the FortiGate-VM Instance on AVX1

To configure the FortiGate-VM VA instance on AVX1, follow these steps:

1. Login into the FG-1 console with the username "admin". You can use the AVX WebUI VA console or the AVX VA console option. By default, there is no password. Just press **Enter**.
2. The AVX ports do not map identically to the ports on the FortiGate-VM instance. Conduct a check to confirm correct port numbering and MAC addresses using the "get hardware nic portX" command on the FG-1 console.
3. Configure the network settings (management = port2, ingress = port3, egress = port4) as follows:

```
config system interface
```

```
edit "port2"
```

```
set ip 10.10.152.123 255.255.255.0 (use your own IP address)
```

```
set allowaccess ping https ssh http fgfm
```

```
next
```

```
edit "port3"
```

```
set ip 192.168.1.51 255.255.255.0 (use your own IP address)
```

```
set allowaccess ping https ssh http fgfm
```

```
next
```

```
edit "port4"
```

```
set ip 192.168.2.51 255.255.255.0 (use your own IP address)
```

```
set allowaccess ping https ssh http fgfm
```

```
end
```

4. Configure the network gateway as follows:

```
config router static
```

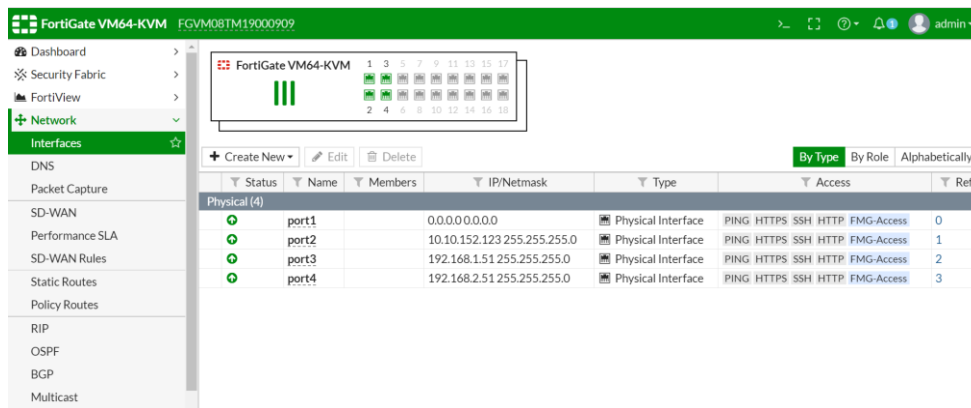
```
edit 1
```

```
set device "port2"
```

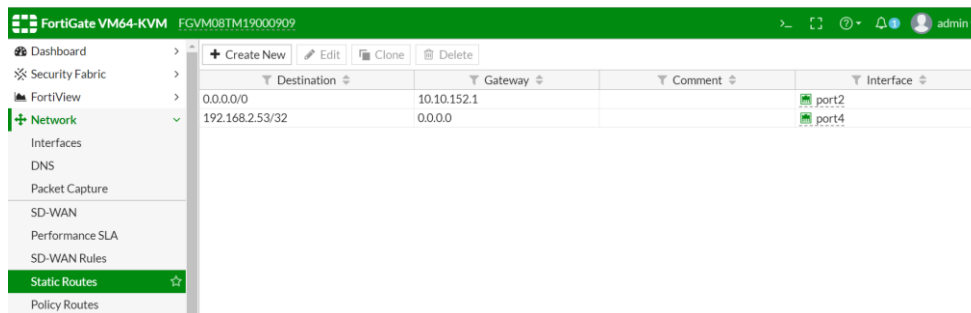
```
set gateway 10.10.152.1 (use your own gateway IP)
```

```
end
```

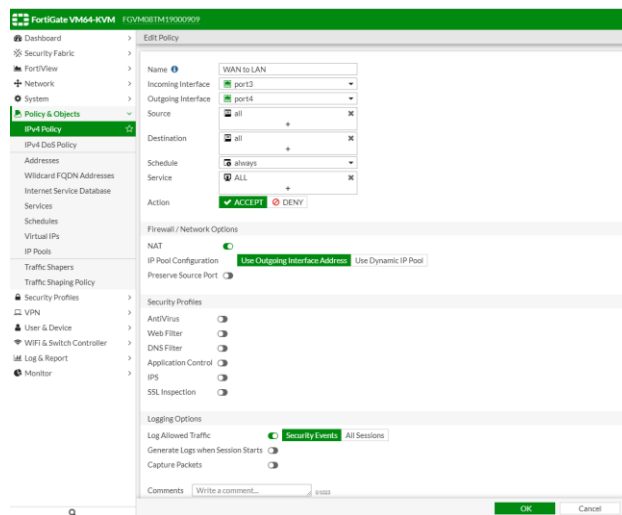
5. Login to the FG-1 WebUI with the default admin credentials.
6. Apply a **valid FortiGate-VM license** (from Fortinet) to proceed.
7. Login again into the FG-1 WebUI and confirm the network settings for port2, port3 and port4.



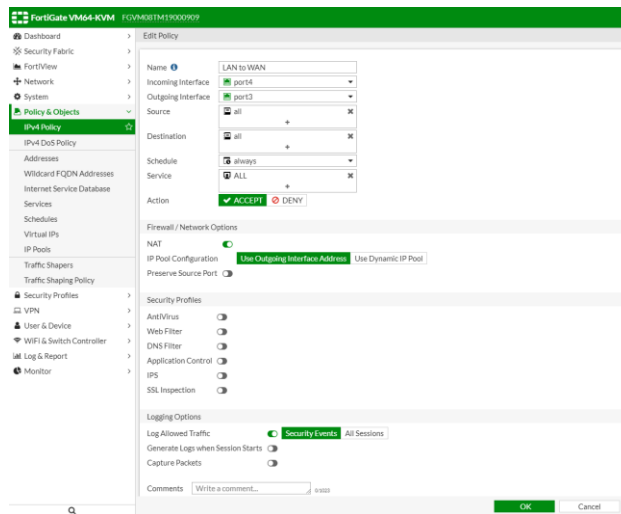
8. Add the following Static Routes:



9. Configure the IPV4 Policy for port3 (WAN) to port4 (LAN) traffic as follows:



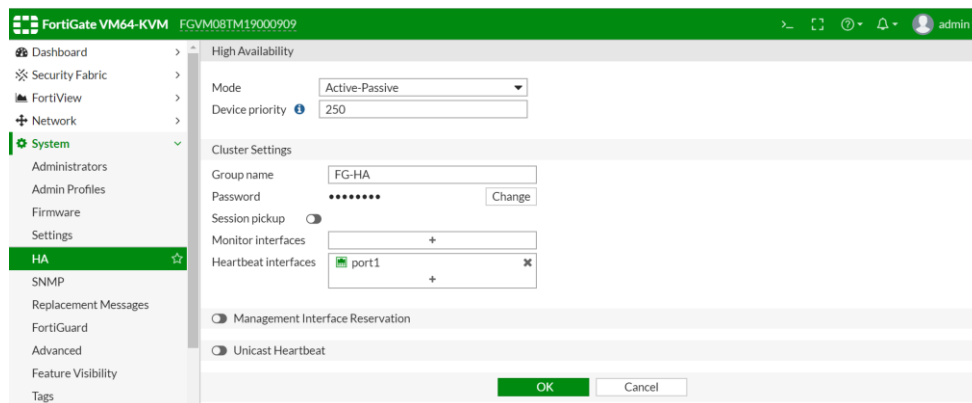
10. Configure the IPV4 Policy for port4 (LAN) to port3 (WAN) traffic as follows:



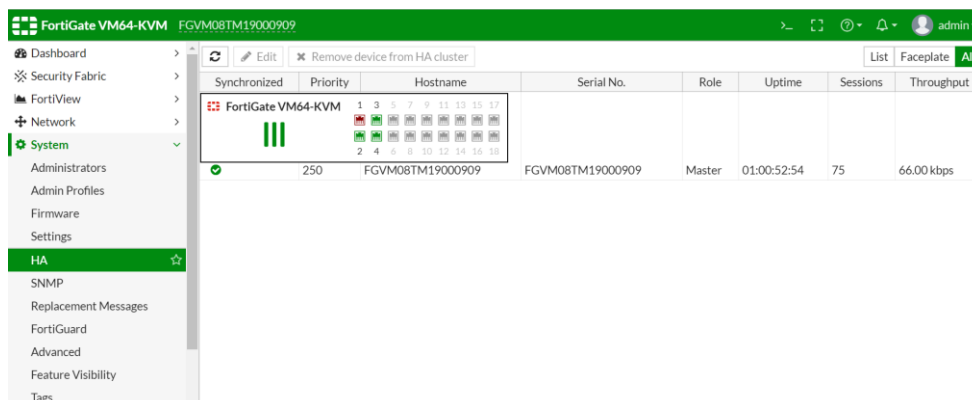
11. Configure HA by navigating to System > HA.

- Mode = Active-Passive
- Device priority = 250 (*higher value to indicate the Master*)
- Group name = FG-HA (*or name of your own choice*)
- Password (*your own choice*)
- Heartbeat interfaces = port1

This FortiGate-VM will be the Master/Active device.



12. Click on OK. FG-1 on AVX1 is the first member and Master of the HA cluster.



## 7. Configuring AVX2

To configure the second AVX appliance, repeat the same steps from section 4 Configuring AVX1 with the only difference in steps 4-5.

4. Change hostname to AVX2.

```
AN(config)#hostname AVX2
```

```
AVX2(config)#
```

5. Configure IP address and default gateway for the management port.

```
AVX2(config)#ip address 10.10.152.172 255.255.255.0 (use your own IP)
```

```
AVX2(config)#ip route default 10.10.152.1 (use your own gateway IP)
```

After step 7 is completed, you may now access the AVX2 appliance using the WebUI at <https://<IP>:8888>. For our example, <https://10.10.152.172:8888>.

## 8. Deploying the FortiGate-VM Instance on AVX2

To deploy the FortiGate-VM instance on the second AVX appliance, AVX2, repeat the same steps from section 5 Deploying the FortiGate-VM instance on AVX1.

Note that the AVX2 WebUI will have a different management IP address than AVX1.

## 9. Configuring the FortiGate-VM Instance on AVX2

To complete the FortiGate-VM configuration, repeat the same steps from section 6 Configuring the FortiGate-VM instance on AVX1 with the only difference in steps 3 (edit port2), and 11-12.

3. Configure the network settings (management = port2, ingress = port3, egress = port4) as follows:

```
config system interface
```

```
edit "port2"
```

```
set ip 10.10.152.124 255.255.255.0 (use your own IP)
```

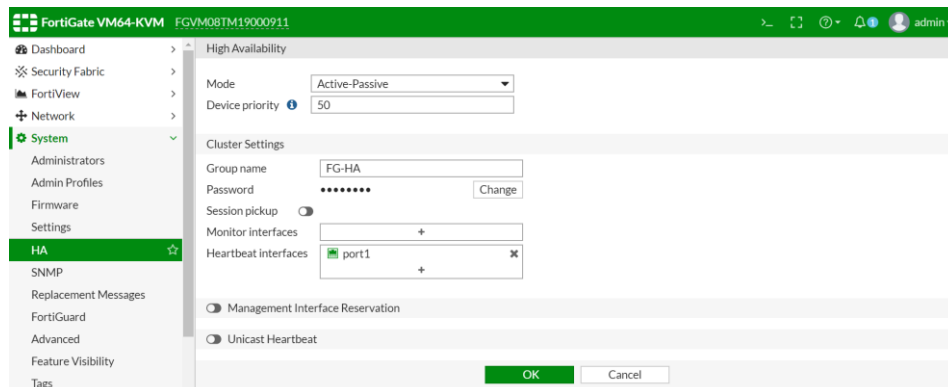
```
set allowaccess ping https ssh http fgfm
```

```
end
```

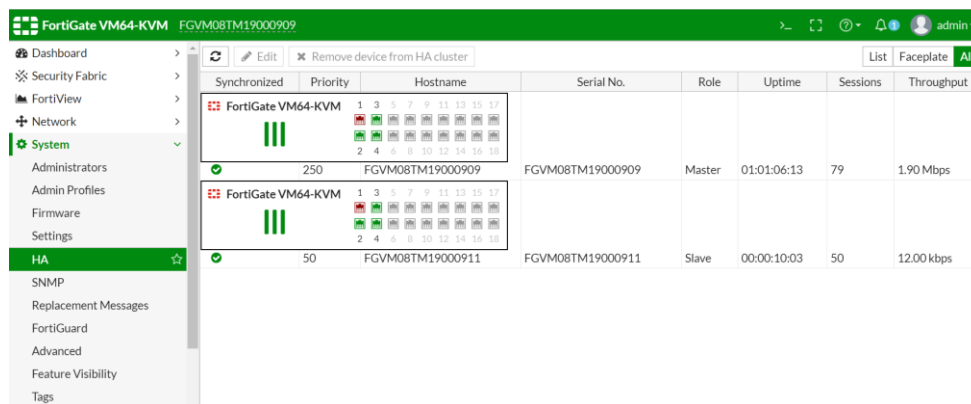
11. Configure HA by navigating to System > HA.

- a. Mode = Active-Passive
- b. Device priority = 50 (*lower value than the Master 250*)
- c. Group name = (*same name used for FG-1 on AVX1*)
- d. Password (*your own choice*)
- e. Heartbeat interfaces = port1



This FortiGate-VM will be the Slave/Passive device.



12. Click on OK. The process will take a few minutes and you will lose connectivity to the WebUI. You will need to login again to FG-1 on AVX1 to view the HA status. When complete, FG-1 on AVX2 is the second member and Slave of the HA cluster.



The screenshot shows the FortiGate VM64-KVM HA status page. The left sidebar contains a menu with options: Dashboard, Security Fabric, FortiView, Network, System (selected), Administrators, Admin Profiles, Firmware, Settings, HA (highlighted), SNMP, Replacement Messages, FortiGuard, Advanced, Feature Visibility, and Tags. The main content area displays a table of HA cluster members. The table has columns: Synchronized, Priority, Hostname, Serial No., Role, Uptime, Sessions, and Throughput. There are two entries: a Master device (FGVM08TM19000909) and a Slave device (FGVM08TM19000911). Each entry has a status icon (green checkmark) and a small table of 17 columns representing different interfaces.

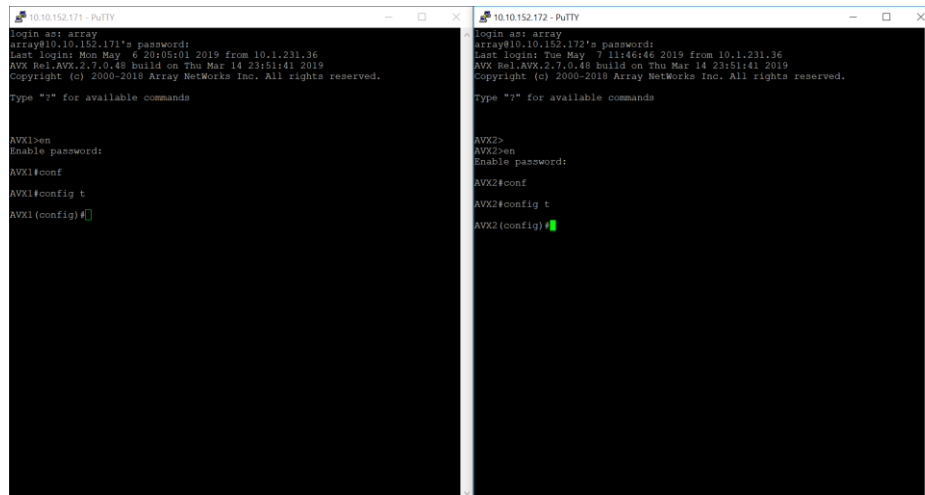
Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
	250	FGVM08TM19000909	FGVM08TM19000909	Master	01:01:06:13	79	1.90 Mbps
	50	FGVM08TM19000911	FGVM08TM19000911	Slave	00:00:10:03	50	12.00 kbps



## 10. Verifying the FortiGate-VM HA on AVX Configuration

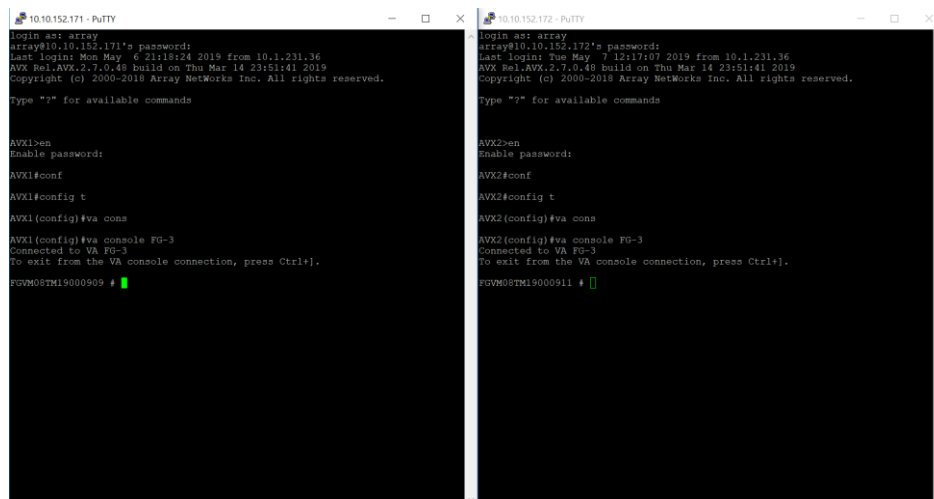
To test and verify that the FortiGate-VM HA on AVX configuration is working, you must now simulate a failure of the master or active FortiGate-VM over to the slave or passive FortiGate-VM.

1. Login to the console on both AVX1 and AVX2.



The image shows two terminal windows side-by-side. The left window is titled '10.10.152.171 - PuTTY' and the right is '10.10.152.172 - PuTTY'. Both show a login prompt for 'array' with IP '10.10.152.171' and '10.10.152.172' respectively. After logging in, the user enters 'AVX1>en' and 'AVX2>en' to enable the password. Then, they enter 'AVX1#conf' and 'AVX2#conf' to enter configuration mode. Finally, they enter 'AVX1(config)#' and 'AVX2(config)#' to reach the configuration prompt.

2. Login to FG-1 console on both AVX1 and AVX2.



The image shows two terminal windows side-by-side. The left window is titled '10.10.152.171 - PuTTY' and the right is '10.10.152.172 - PuTTY'. Both show the same login and configuration steps as the previous image. After reaching the configuration prompt, the user enters 'AVX1(config)#va cons' and 'AVX2(config)#va cons' to enter the virtual console mode. Then, they enter 'AVX1(config)#va console FG-3' and 'AVX2(config)#va console FG-3' to connect to the FG-3 console. Finally, they enter 'FGVM08TM19000909 #' and 'FGVM08TM19000911 #' to reach the FG-3 console prompt.

3. Type "get system ha status" to obtain the HA status of the cluster.

```
FGVM08TM19000909 # get system ha status
HA Health Status: OK
Model: FortiGate-VN64-KVM
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 4 days 20:43:46
Cluster state change time: 2019-05-06 20:52:27
Master selected using:
<2019/05/06 20:52:27> FGVM08TM19000909 is selected as the master because
it has the largest value of uptime.
<2019/05/06 04:06:47> FGVM08TM19000909 is selected as the master because
it has the largest value of uptime.
<2019/05/06 03:59:12> FGVM08TM19000909 is selected as the master because
it's the only member in the cluster.
sea_pickup: disable
override: disable
Configuration Status:
FGVM08TM19000909(updated 4 seconds ago): in-sync
FGVM08TM19000911(updated 1 seconds ago): in-sync
System Usage status:
FGVM08TM19000909(updated 4 seconds ago):
sessions=3, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=1
FGVM08TM19000911(updated 1 seconds ago):
sessions=0, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=1
HBBDEV status:
FGVM08TM19000909(updated 4 seconds ago):
port1: physical/10000full, up, rx-bytes/packets/dropped/errors=151390
155/566594/0/0, tx=24247888/599097/0/0
FGVM08TM19000911(updated 1 seconds ago):
port1: physical/10000full, up, rx-bytes/packets/dropped/errors=496984
5/14054/0/0, tx=319855/11933/0/0
Master: FGVM08TM19000909, operating cluster index = 1
Slave: FGVM08TM19000911, operating cluster index = 0
number of volcluster: 1
volcluster 1: work 169.254.0.2
FGVM08TM19000909 # exec reboot
This operation will reboot the system !
Do you want to continue? (y/n)y
System is rebooting...
The system is going down NOW !!
FGVM08TM19000909 #
```

```
FGVM08TM19000911 login: admin
Password:
Welcome !
FGVM08TM19000911 # get system ha status
HA Health Status: OK
Model: FortiGate-VN64-KVM
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 4 days 20:43:32
Cluster state change time: 2019-05-07 11:53:37
Master selected using:
<2019/05/07 11:53:37> FGVM08TM19000909 is selected as the master because
it has the largest value of uptime.
sea_pickup: disable
override: disable
Configuration Status:
FGVM08TM19000911(updated 2 seconds ago): in-sync
FGVM08TM19000909(updated 0 seconds ago): in-sync
System Usage status:
FGVM08TM19000911(updated 2 seconds ago):
sessions=0, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=1
FGVM08TM19000909(updated 0 seconds ago):
sessions=3, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=1
HBBDEV status:
FGVM08TM19000911(updated 2 seconds ago):
port1: physical/10000full, up, rx-bytes/packets/dropped/errors=494318
2/1364/0/0, tx=3295508/11844/0/0
FGVM08TM19000909(updated 0 seconds ago):
port1: physical/10000full, up, rx-bytes/packets/dropped/errors=151374
437/566594/0/0, tx=24247888/599097/0/0
Master: FGVM08TM19000909, operating cluster index = 1
Slave: FGVM08TM19000911, operating cluster index = 0
number of volcluster: 1
volcluster 1: standby 169.254.0.2
FGVM08TM19000909, operating cluster index = 0
FGVM08TM19000911, operating cluster index = 1
FGVM08TM19000911 #
```

Note that the Master is FGVM08TM19000909 on AVX1 (left-hand side) and the Slave is FGVM08TM19000911 on AVX2 (right-hand side).

- Now force a failure by rebooting the Master on AVX1 and checking the status on AVX2.

```
FGVM08TM19000909 # get system ha status
HA Health Status: OK
Model: FortiGate-VN64-KVM
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 4 days 20:48:17
Cluster state change time: 2019-05-06 21:28:13
Master selected using:
<2019/05/06 21:28:13> FGVM08TM19000911 is selected as the master because
the peer member FGVM08TM19000909 has SET AS_SLAVE flag set.
<2019/05/07 11:53:37> FGVM08TM19000909 is selected as the master because
it has the largest value of uptime.
sea_pickup: disable
override: disable
Configuration Status:
FGVM08TM19000911(updated 2 seconds ago): in-sync
FGVM08TM19000909(updated 5 seconds ago): in-sync
System Usage status:
FGVM08TM19000911(updated 2 seconds ago):
sessions=6, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=1
FGVM08TM19000909(updated 5 seconds ago):
sessions=3, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=1
HBBDEV status:
FGVM08TM19000911(updated 2 seconds ago):
port1: physical/10000full, up, rx-bytes/packets/dropped/errors=556758
0/15736/0/0, tx=1777455/13583/0/0
FGVM08TM19000909(updated 5 seconds ago):
port1: physical/10000full, up, rx-bytes/packets/dropped/errors=151835
0/6/566224/0/0, tx=24247888/599097/0/0
Master: FGVM08TM19000911, operating cluster index = 1
Slave: FGVM08TM19000909, operating cluster index = 0
number of volcluster: 1
volcluster 1: work 169.254.0.1
Master: FGVM08TM19000911, operating cluster index = 0
Slave: FGVM08TM19000909, operating cluster index = 1
FGVM08TM19000911 #
```

Note that the new Master is FGVM08TM19000911 on AVX2 (right-hand side).

- When the FGVM08TM19000909 on AVX1 (left-hand side) boots back up successfully, it will resume ownership as the Master.

```
FGVM08TM19000909 login: admin
Password:
Welcome !
FGVM08TM19000909 # get system ha status
HA Health Status: OK
Model: FortiGate-VN64-KVM
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 4 days 20:50:0
Cluster state change time: 2019-05-06 21:28:58
Master selected using:
<2019/05/06 21:28:58> FGVM08TM19000909 is selected as the master because
it has the largest value of uptime.
sea_pickup: disable
override: disable
Configuration Status:
FGVM08TM19000909(updated 0 seconds ago): in-sync
FGVM08TM19000911(updated 4 seconds ago): in-sync
System Usage status:
FGVM08TM19000909(updated 0 seconds ago):
sessions=17, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=1
FGVM08TM19000911(updated 4 seconds ago):
sessions=12, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=1
HBBDEV status:
FGVM08TM19000909(updated 0 seconds ago):
port1: physical/10000full, up, rx-bytes/packets/dropped/errors=152939
535/0/0, tx=143454/459/0/0
FGVM08TM19000911(updated 4 seconds ago):
port1: physical/10000full, up, rx-bytes/packets/dropped/errors=573481
0/16232/0/0, tx=24247888/599097/0/0
Master: FGVM08TM19000909, operating cluster index = 1
Slave: FGVM08TM19000911, operating cluster index = 0
number of volcluster: 1
volcluster 1: work 169.254.0.2
Master: FGVM08TM19000909, operating cluster index = 1
Slave: FGVM08TM19000911, operating cluster index = 0
FGVM08TM19000909 #
```

```
FGVM08TM19000911 # get system ha status
HA Health Status: OK
Model: FortiGate-VN64-KVM
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 4 days 20:49:36
Cluster state change time: 2019-05-06 21:28:57
Master selected using:
<2019/05/06 21:28:57> FGVM08TM19000909 is selected as the master because
it has the largest value of uptime.
<2019/05/06 21:28:13> FGVM08TM19000911 is selected as the master because
it's the only member in the cluster.
<2019/05/06 21:28:13> FGVM08TM19000911 is selected as the master because
the peer member FGVM08TM19000909 has SET AS_SLAVE flag set.
<2019/05/07 11:53:37> FGVM08TM19000909 is selected as the master because
it has the largest value of uptime.
sea_pickup: disable
override: disable
Configuration Status:
FGVM08TM19000911(updated 1 seconds ago): in-sync
FGVM08TM19000909(updated 2 seconds ago): in-sync
System Usage status:
FGVM08TM19000911(updated 1 seconds ago):
sessions=12, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=1
FGVM08TM19000909(updated 2 seconds ago):
sessions=17, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=1
HBBDEV status:
FGVM08TM19000911(updated 1 seconds ago):
port1: physical/10000full, up, rx-bytes/packets/dropped/errors=567504
2/16101/0/0, tx=2331573/14135/0/0
FGVM08TM19000909(updated 2 seconds ago):
port1: physical/10000full, up, rx-bytes/packets/dropped/errors=111594
433/0/0, tx=24247888/599097/0/0
Master: FGVM08TM19000911, operating cluster index = 0
Slave: FGVM08TM19000909, operating cluster index = 1
number of volcluster: 1
volcluster 1: standby 169.254.0.2
Slave: FGVM08TM19000911, operating cluster index = 1
Master: FGVM08TM19000909, operating cluster index = 0
FGVM08TM19000911 #
```

## 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