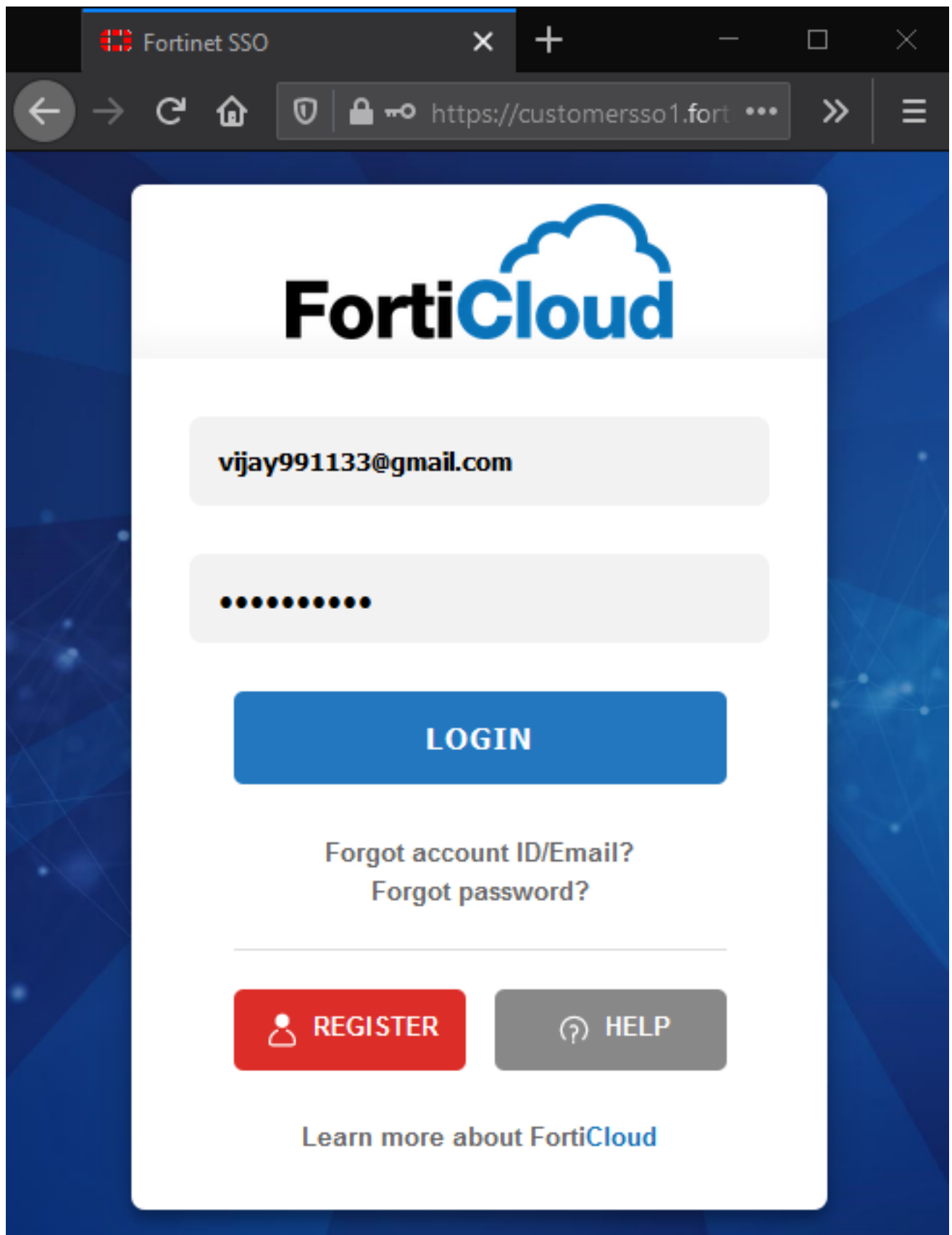


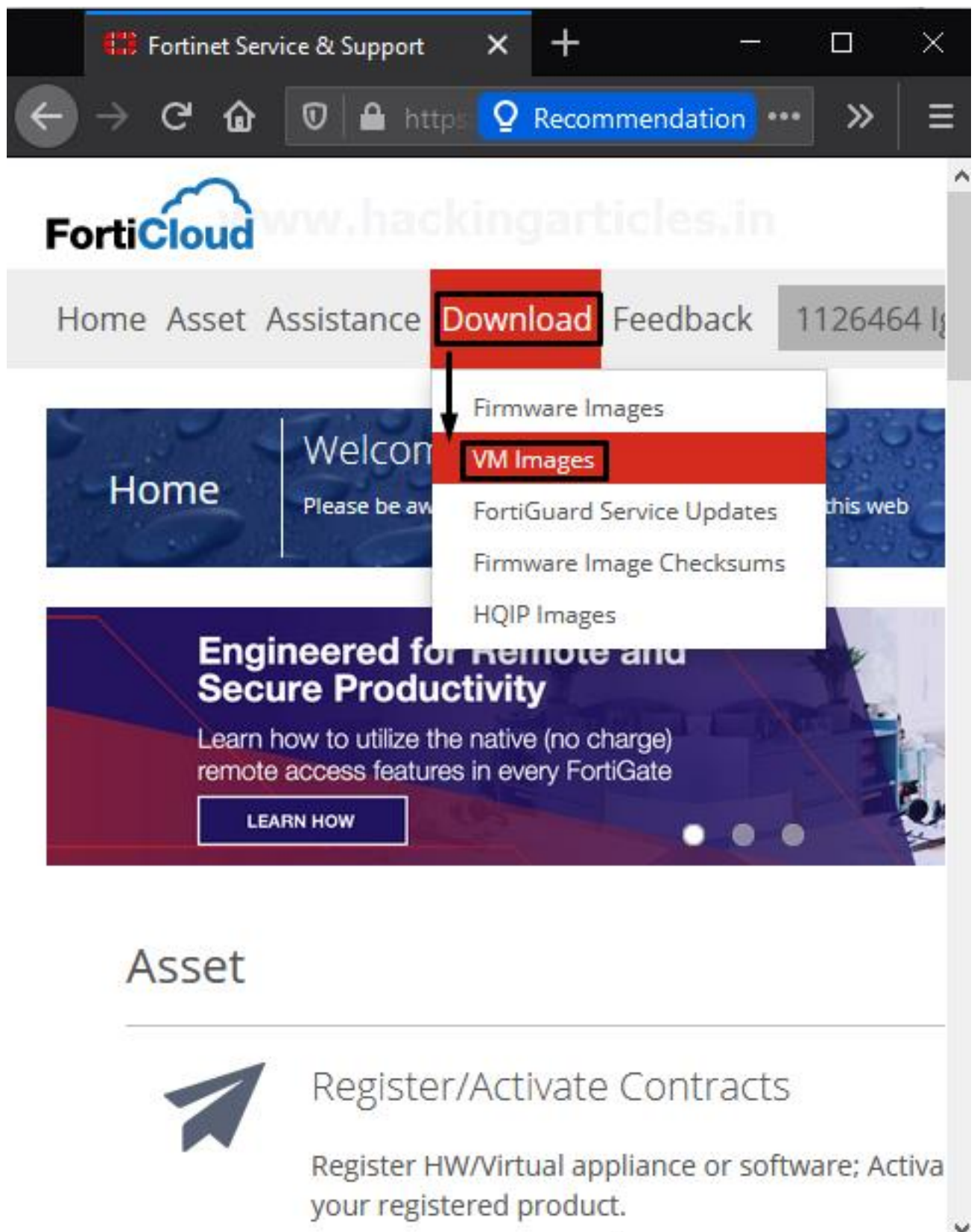
Firewall Lab Setup : FortiGate

1. Download FortiGate Virtual firewall

First, we need to download the virtual FortiGate Firewall from the official FortiGate portal.



By creating an account or log in to the account go to **Download > VM Images** as shown in the image below.



Further then Select Product: **FortiGate** > Select Platform: **VMWare ESXi** as shown in the image below. By default, you don't have any license associated with your virtual image so, you can go with the trial version or you can buy the license as per your requirement.

Select Product

FortiGate

Select Platform

VMWare ESXi

-- Latest Version

6.4.3

6.2.5

-- Earlier Versions

6.4.2

6.2.4

FortiGate for VMWare ESXi









6.4.3

Upgrade Path

File Information	Checksum
Upgrade from previous version of FortiGate for VMware FGT_VM64-v6-build1778-FORTINET.out (67.5 MB)	6dd573b1efd85c6c3467ff938 (SHA-512)
Download	
New deployment of FortiGate for VMware FGT_VM64-v6-build1778-FORTINET.out.ovf.zip (66.96 MB)	0beb04052bf0b762e9a699cc (SHA-512)
Download	

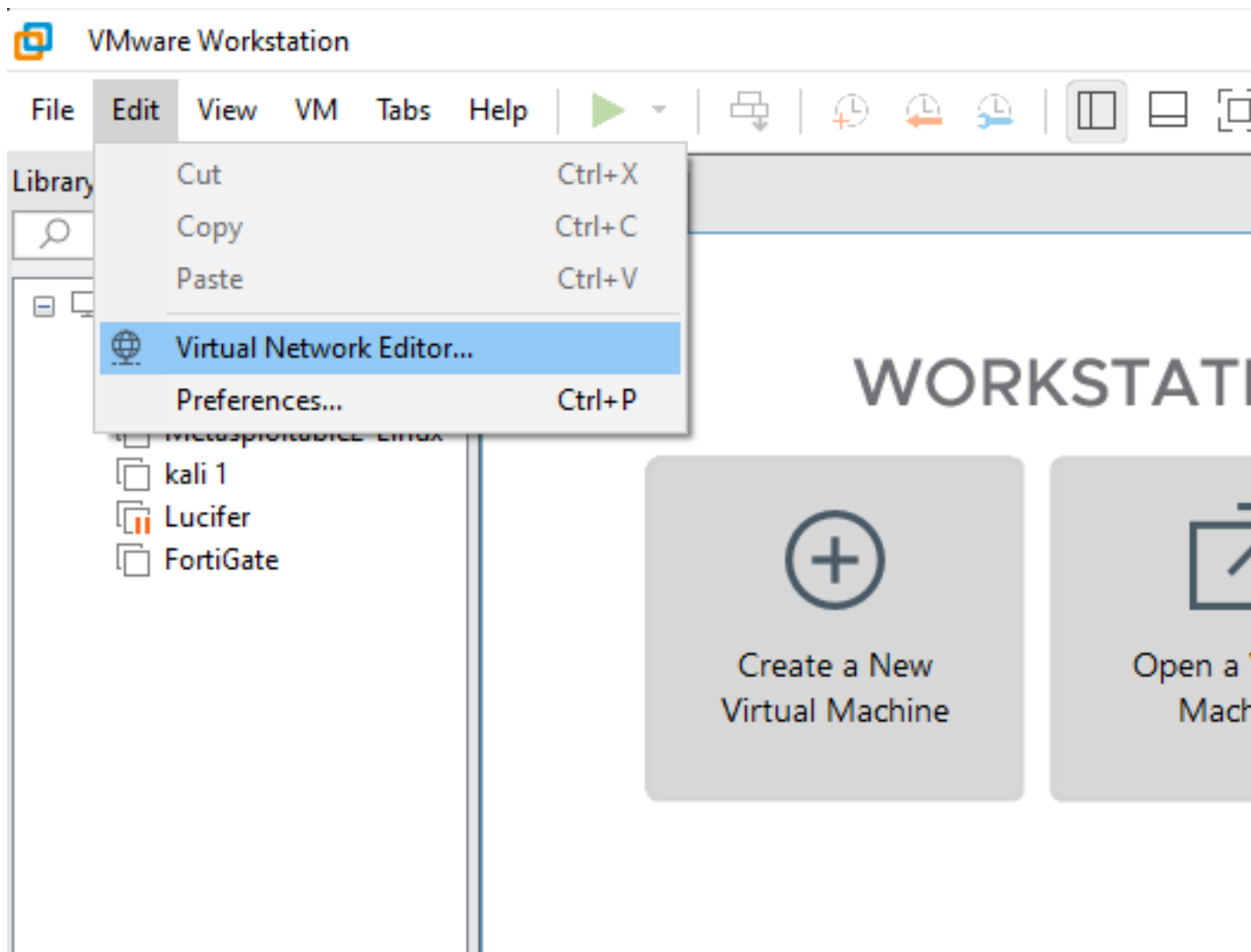
After downloading the compressed FortiGate VM file you need to extract the compressed Zip file by using your favourite extractor and the extracted Zip file similarly looks like the below image.

This PC > Downloads > FGT_VM64-v6-build1778-FORTINET.out.ovf

Name	Date modified	Type
 datadrive	23-08-2010 23:02	VMDK File
 FortiGate-VM64.hw07_vmxnet3	22-10-2020 02:32	Open Virtu
 FortiGate-VM64.hw13	22-10-2020 02:32	Open Virtu
 FortiGate-VM64.hw14	22-10-2020 02:32	Open Virtu
 FortiGate-VM64.nsxt	22-10-2020 02:32	Open Virtu
 FortiGate-VM64	22-10-2020 02:32	Open Virtu
 FortiGate-VM64.vapp	22-10-2020 02:32	Open Virtu
 fortios	22-10-2020 02:32	VMDK File

2. Configure Virtual network interfaces for FortiGate

Let's configure Virtual Network Adaptors as per your requirements. To do this open VMware then go to Edit > Virtual Network Editor as shown in the image below



Further, then it will open another prompt that allows you to modify the network configuration. To make changes in network configuration it needs the Administrator privileges to provide Admin privileges click on change settings as shown below

The screenshot shows the VMware Network Editor window for VMnet0. At the top, there are buttons for 'Add Network...', 'Remove Network', and 'Rename Network'. The 'VMnet Information' section has three radio buttons: 'Bridged (connect VMs directly to the external network)', 'NAT (shared host's IP address with VMs)', and 'Host-only (connect VMs internally in a private network)'. The 'Host-only' option is selected. Below these are checkboxes for 'Connect a host virtual adapter to this network' (checked) and 'Use local DHCP service to distribute IP address to VMs' (checked). The 'Host virtual adapter name' is 'VMware Network Adapter VMnet0'. At the bottom, 'Subnet IP' is '192.168.200.0' and 'Subnet mask' is '255.255.255.0'. A warning message at the bottom states 'Administrator privileges are required to modify the network configuration' with a 'Change Settings' button highlighted by a red box. Other buttons at the bottom include 'Restore Defaults', 'Import...', 'Export...', 'OK', 'Cancel', and 'Apply'.

Or also you can directly access the Virtual network editor app by click on Windows Start Button and search for Virtual Network Editor. If you are using Linux (i.e. Ubuntu) you can type the below command to open Virtual Network Editor.

```
sudo vmware-netcfg
```

By default, there are only two virtual network interfaces, i.e., *VMNet1* and *VMNet8*. So, click on the Add Network and make your virtual interface host only. After that, you have to provide a unique IP address of network devices to each network interface. For example, I am going to use 192.168.200.0/24 for the vmnet0 interface and so on...

Use Ip of your network devices or whatever as per your requirement. Similarly, you can add as much as network interfaces as you want but remember one thing all network configuration should be configured to Host-only and you can enable or disable DHCP service as per you system requirement

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Host-only	-	Connected	Enabled	192.168.200.0
VMnet1	Host-only	-	Connected	Enabled	192.168.16.0
VMnet2	Host-only	-	Connected	-	192.168.137.0
VMnet3	Host-only	-	Connected	Enabled	192.168.70.0
VMnet4	Host-only	-	Connected	Enabled	192.168.80.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.232.0
VMnet11	Host-only	-	Connected	-	192.168.237.0
VMnet12	Host-only	-	Connected	Enabled	10.1.20.0

Add Network...

Remove Network

Renam

VMnet Information

☐ Bridged (connect VMs directly to the external network)

Bridged to:

Automatic

☐ NAT (shared host's IP address with VMs)

NAT Set

☒ Host-only (connect VMs internally in a private network)

☒ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet0

☒ Use local DHCP service to distribute IP address to VMs

DHCP Se

Subnet IP: 192 . 168 . 200 . 0

Subnet mask: 255 . 255 . 255 . 0

Restore Defaults

Import...

Export...

OK

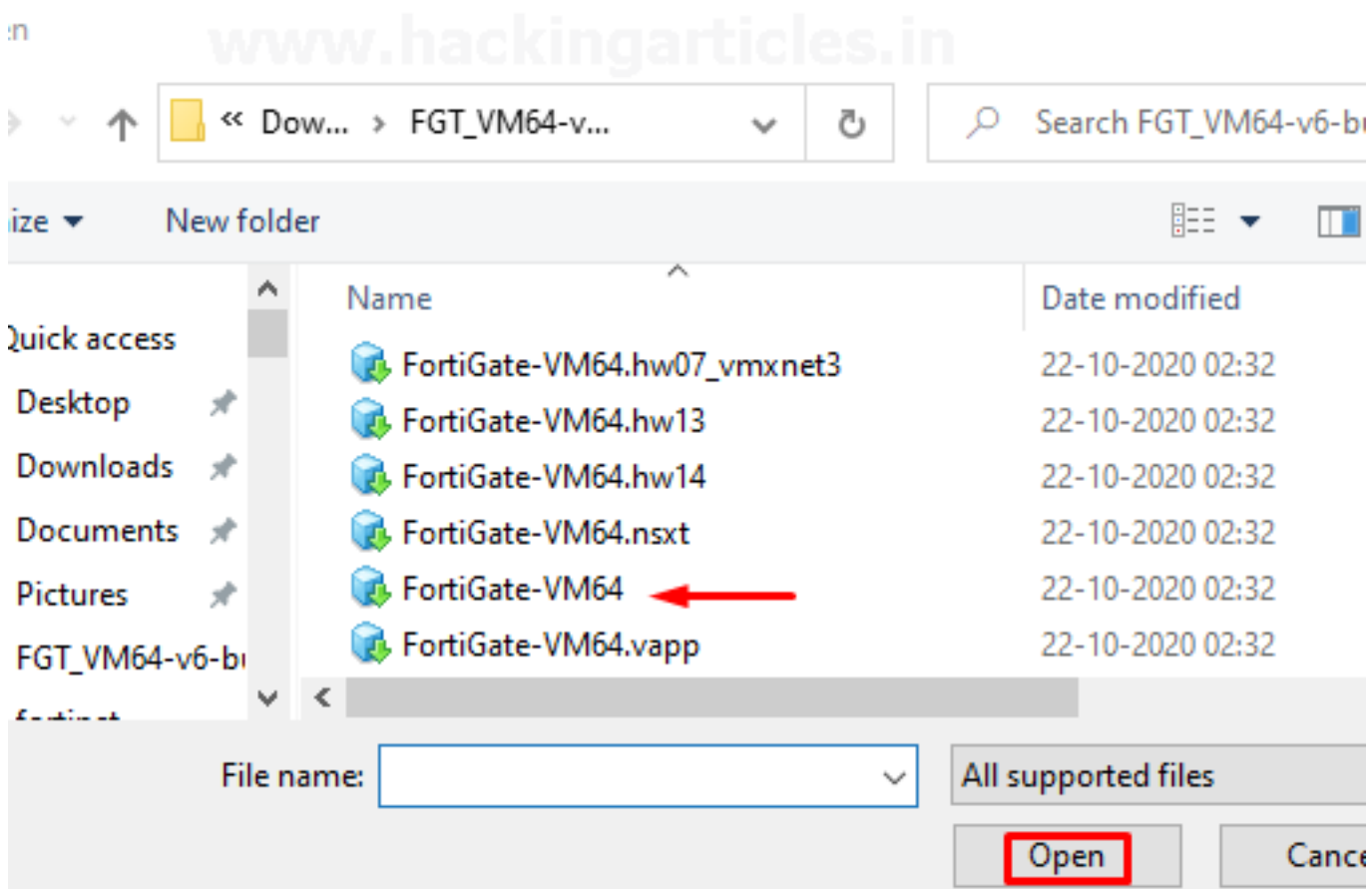
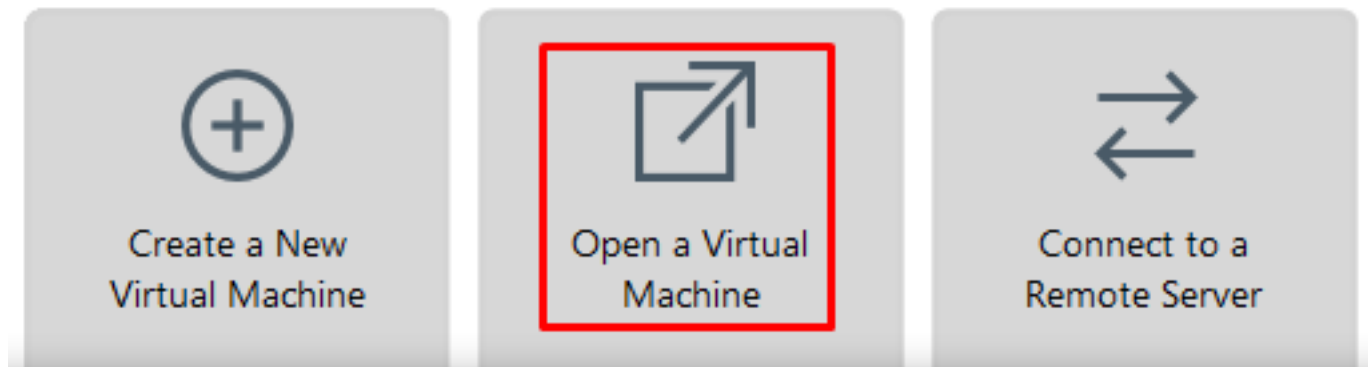
Cancel

Apply

3. Deployment of FortiGate VM image in VMWare

Now it's time to deploy the FortiGate virtual firewall in VMWare Workstation. Just open the VMWare Workstation and go to **Files >> Open** (Ctrl+O) or go to the Home tab and select open a virtual Machine. Select the FortiGate-VM64.ovf file that you have downloaded from the official Website of FortiGate as shown below

WORKSTATION 16 PRO™



Then after it will open another prompt of End User License Agreement accept it and move to next

Import Virtual Machine

×

End User License Agreement
Accept the end user license agreements.

End User License Agreement for FortiGate Virtual Appliance

NOTICE TO ALL USERS: PLEASE READ THE TERMS AND CONDITIONS OF LICENSE AGREEMENT CAREFULLY. FORTINET, INC. IS WILLING TO LICENSE SOFTWARE TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE TO THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS LICENSE AGREEMENT AND DO NOT INSTALL THE SOFTWARE. IF YOU PURCHASED THE SOFTWARE ON TANGIBLE MEDIA (e.g., CD-ROM) WITHOUT THE OPPORTUNITY TO REVIEW THIS LICENSE AND YOU DO NOT AGREE TO THIS LICENSE AGREEMENT, YOU MAY OBTAIN A REFUND OF THE AMOUNT ORIGINALLY PAID IF YOU: (A) DO NOT USE THE SOFTWARE AND (B) RETURN IT WITH PROOF OF PAYMENT, WITHIN THIRTY (30) DAYS OF THE PURCHASE DATE TO THE LOCATION FROM WHICH IT WAS OBTAINED.

This End User License Agreement (EULA) is an agreement between you and Fortinet, Inc.

☒ I accept the terms of the license agreement.

Help

< Back

Next >

Cancel

On the next prompt Assign a Name for the new Virtual machine and a Storage Path then after select import as shown below

Import Virtual Machine

×

Store the new Virtual Machine
Provide a name and local storage path for the new virtual machine.

www.hackingarticles.in

Name for the new virtual machine:

FortiGate-VM64

Storage path for the new virtual machine:

C:\Users\vijvi\OneDrive\Documents\Virtual Machines\FortiGate

Browse...

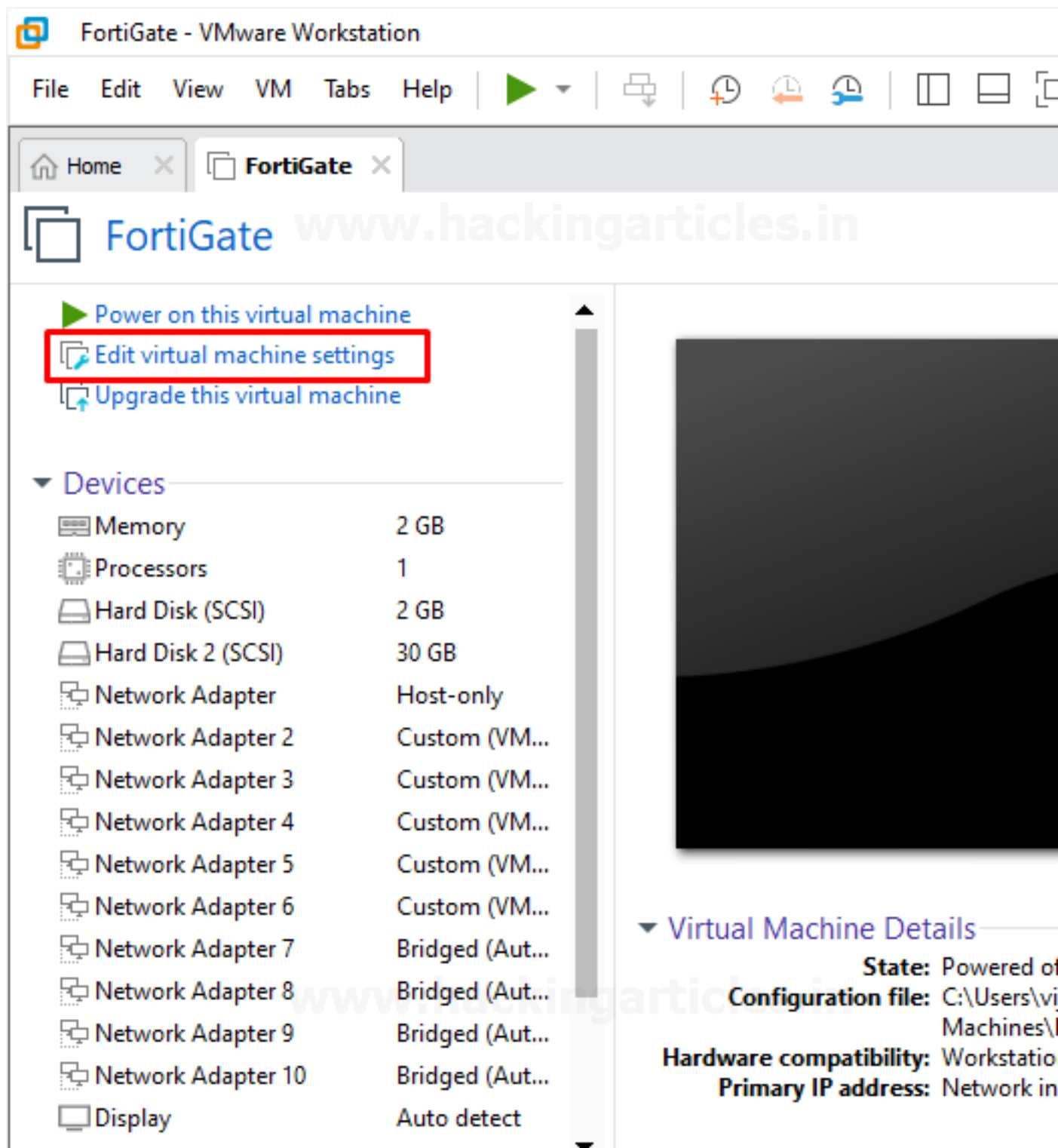
Help

< Back

Import

Cancel

This process going to take some time, so have *patience*. After the successful completion of this process. Now it's time to configure the Virtual Firewall resources by clicking on Edit virtual machine settings. just modify the assigned virtual network interfaces, memory, and processor by going to Edit virtual machine.



In my case, I'm giving 2GB RAM, 30 GB of Hard Disk, 1 Processor, and 6 different virtual network interfaces (VMNet2, VMNet3, VMNet4, VMNet11, VMnet11, VMnet12 to different network adaptors. Check the below image for reference.

Virtual Machine Settings

The screenshot shows the 'Virtual Machine Settings' window with the 'Options' tab selected. The 'Hardware' section on the left lists various components. The 'Network Adapter' section is highlighted with a red box, and 'Network Adapter 2' is selected. A red arrow points from 'Network Adapter 2' to the 'Custom: Specific virtual network' option in the 'Network connection' section on the right.

Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	2 GB
Hard Disk 2 (SCSI)	30 GB
Network Adapter	Host-only
Network Adapter 2	Custom (VMnet2)
Network Adapter 3	Custom (VMnet11)
Network Adapter 4	Custom (VMnet3)
Network Adapter 5	Custom (VMnet4)
Network Adapter 6	Custom (VMnet12)
Network Adapter 7	Bridged (Automatic)
Network Adapter 8	Bridged (Automatic)
Network Adapter 9	Bridged (Automatic)
Network Adapter 10	Bridged (Automatic)
Display	Auto detect

Device status

- ☐ Connected
- ☒ Connect at power on

Network connection

- ☐ Bridged: Connected directly to the physical network
- ☐ Replicate physical network connection
- ☐ NAT: Used to share the host's IP address
- ☐ Host-only: A private network shared with other VMs
- ☒ Custom: Specific virtual network

VMnet2 (Host-only)

☐ LAN segment:

Configuring the Management Interface

We've just finished the deployment process of the FortiGate Firewall in the VMWare workstation. Let's configure an IP Address to the management interface. In manner to assign an IP Address to management interface firstly, we need login to the system with default credentials

Login User: – Admin

Login Password: – In this circumstance, we don't know the default password, Hit enter and change the password as shown below

```
Loading flatkc... ok
Loading /rootfs.gz...ok

Decompressing Linux... Parsing ELF... done.
Booting the kernel.

System is starting...
Serial number is FGUMEV9T3UJPII0A

FortiGate-VM64 login: admin
Password:
You are forced to change your password. Please input a
New Password:
Confirm Password:
Welcome!

FortiGate-VM64 #
```

Let's check the system interfaces by running the following command

```
show system interface
```

```

FortiGate-VM64 # show system interface
name      Name.
fortilink  static  0.0.0.0 0.0.0.0 169.254.1.1 255.255.255.0
aggregate enable
port1     dhcp    0.0.0.0 0.0.0.0 192.168.200.128 255.255.255.0
physical  enable
port2     static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up
port3     static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up
port4     static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up
port5     static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up
port6     static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up
port7     static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up
port8     static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up
port9     static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up
port10    static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up
--More--

```

Port 1 will be for the management interface so, assign a unique IP address to the management port and set to mode static. In this example our IP Address will be 192.168.200.128/24 so, the default gateway will be 192.168.200.1. To assign IP Address to management port run the following command as shown below

```

config system interface
edit port1
set mode static
set ip 192.168.200.128 255.255.255.0
set allowaccess http https telnet ssh ping
end

```

```
FortiGate-VM64 # config system interface ←
FortiGate-VM64 (interface) # edit port1 ←
FortiGate-VM64 (port1) # set mode static ←
FortiGate-VM64 (port1) # set ip 192.168.200.128 255.255.255.0
FortiGate-VM64 (port1) # set allowaccess http https telnet
FortiGate-VM64 (port1) # end ←
FortiGate-VM64 # _
```

Also, we can verify the make changes of system interfaces by running the following command

```
show system interface
```




```
FortiGate-VM64 # show system interface ←
config system interface
  edit "port1"
    set vdom "root"
    set ip 192.168.200.128 255.255.255.0
    set allowaccess ping https ssh http telnet
    set type physical
    set snmp-index 1
  next
  edit "port2"
    set vdom "root"
    set type physical
    set snmp-index 2
  next
  edit "port3"
    set vdom "root"
    set type physical
    set snmp-index 3
  next
  edit "port4"
    set vdom "root"
    set type physical
    set snmp-index 4
  next
--More-- _
```

4. Accessing FortiGate Firewall GUI

Let's check our firewall configuration by accessing the FortiGate Firewall GUI. Before accessing the GUI first, we will check the connectivity to our Firewall using the ping utility by running the following command

```
execute ping 192.268.200.128
```

```
FortiGate-VM64 # execute ping 192.168.200.128   
PING 192.168.200.128 (192.168.200.128): 56 data bytes  
64 bytes from 192.168.200.128: icmp_seq=0 ttl=255 time=  
64 bytes from 192.168.200.128: icmp_seq=1 ttl=255 time=  
64 bytes from 192.168.200.128: icmp_seq=2 ttl=255 time=  
64 bytes from 192.168.200.128: icmp_seq=3 ttl=255 time=  
64 bytes from 192.168.200.128: icmp_seq=4 ttl=255 time=  
  
--- 192.168.200.128 ping statistics ---  
5 packets transmitted, 5 packets received, 0% packet lo  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
  
FortiGate-VM64 #
```

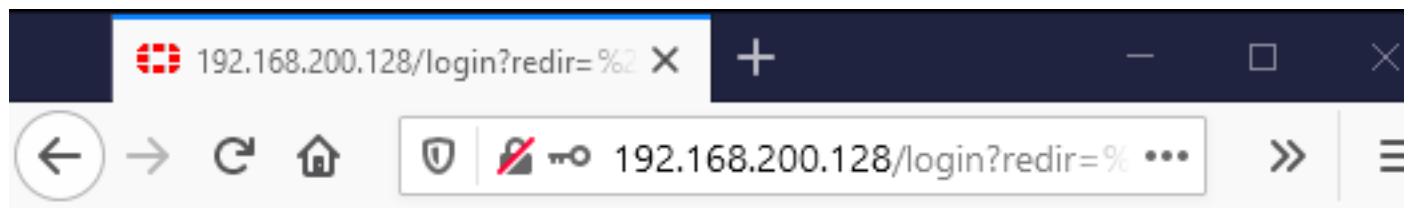
As we can see the IP Address is reachable which means it is working properly now, we will access the FortiGate Firewall GUI using its management interface IP address.

<https://192.168.200.128>

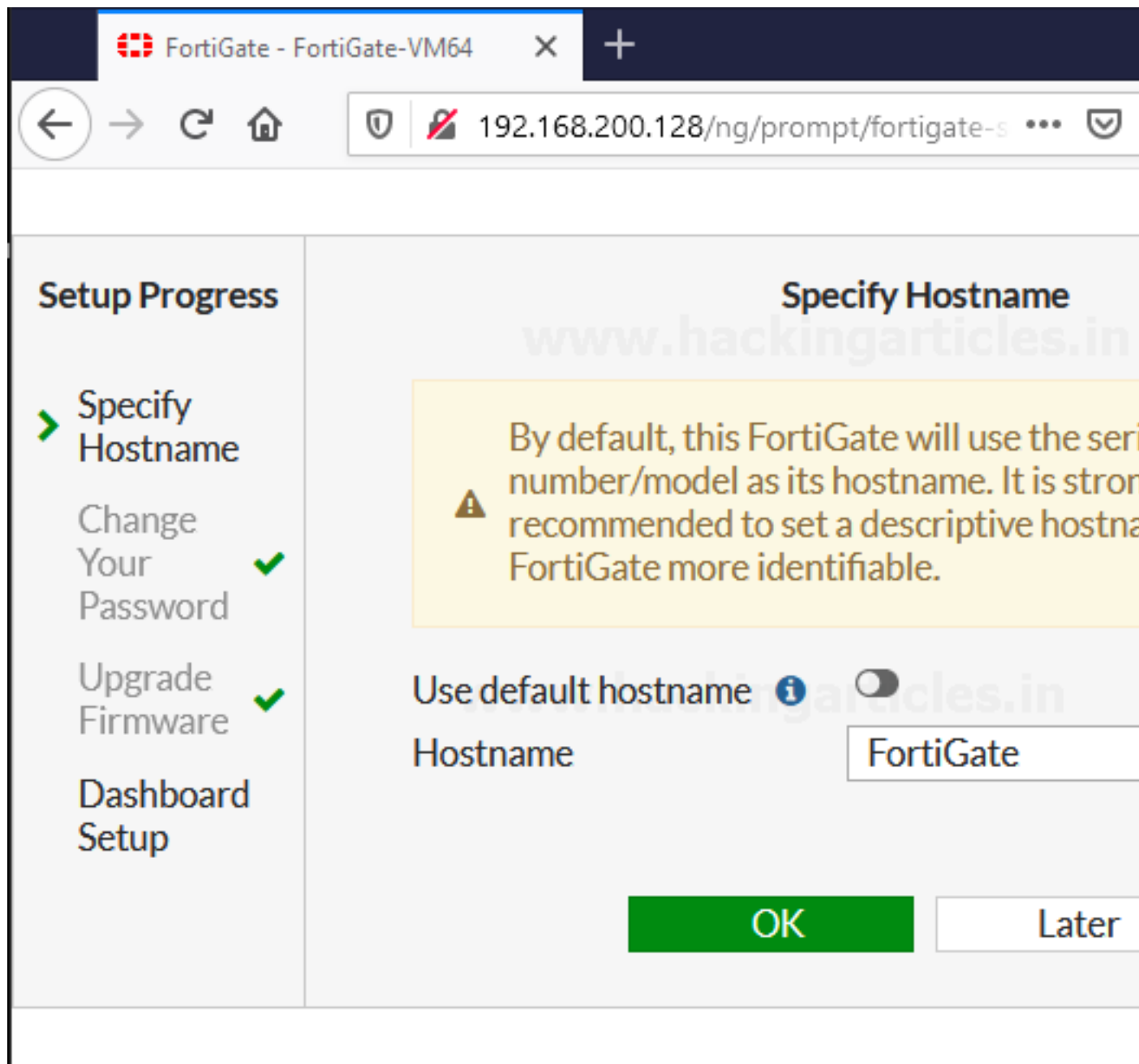
use the same login credential that we have set up on CLI

Username: – admin

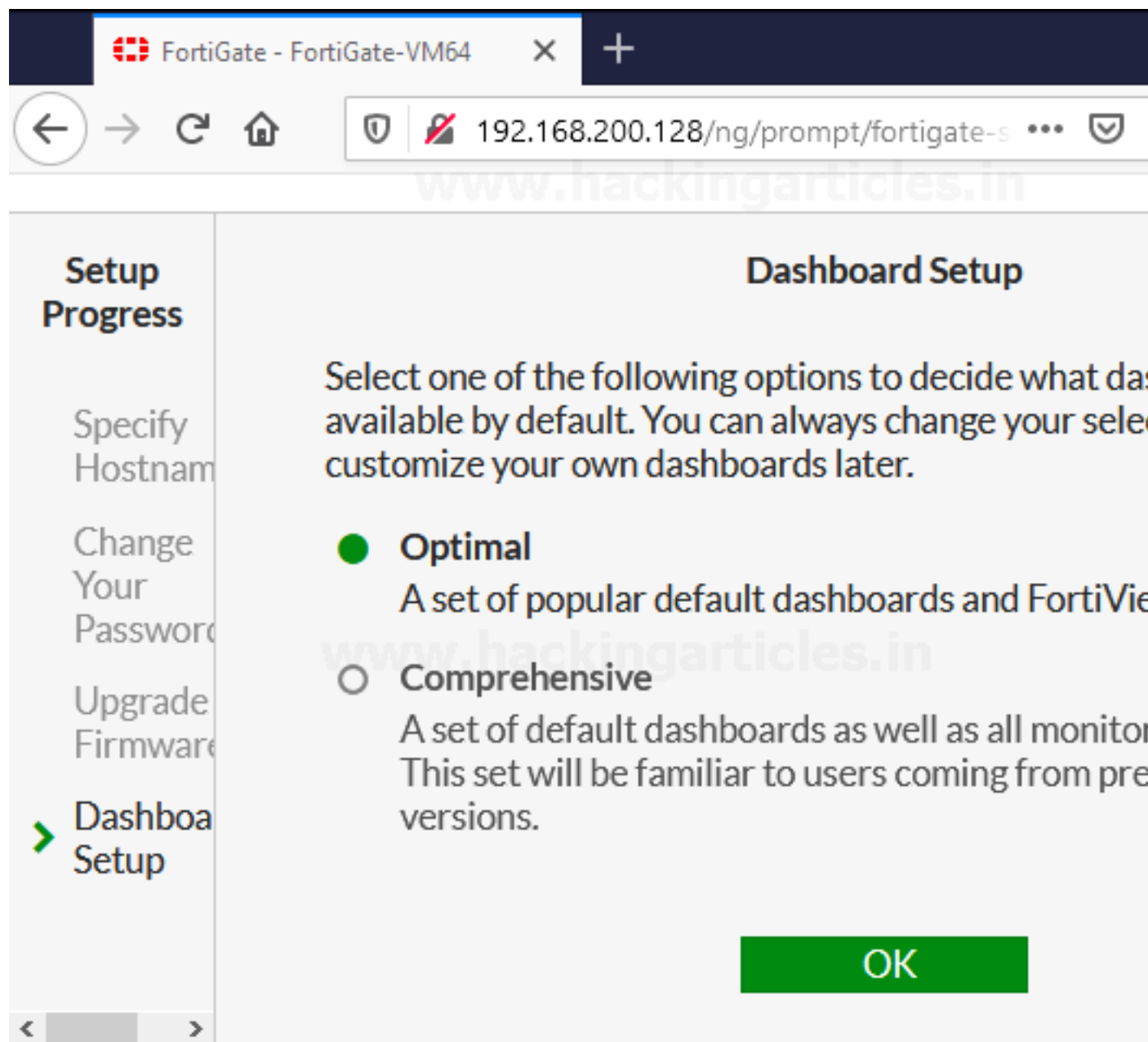
Password: – 123



By logging in to the firewall it will open a setup Prompt where we need to specify the Hostname, change password upgrade firmware, and Dashboard setup By default, this FortiGate will use the serial number/model as its hostname. To make it more identifiable set a descriptive hostname as shown below



Already we have changed the password in Firewall CLI and also, we have already downloaded the latest version of the firewall, so it automatically skips you to the last step to Dashboard setup. Select it to Optimal or Comprehensive as per your requirements



After selecting the type of Dashboard hit ok and finish the setup.

5. GUI Demonstration

The GUI contains the following main menus, which provide access to configuration options for most FortiOS features:

FortiGate - FortiGate-VM64

192.168.200.128/ng/system/dashboard/1

FortiGate VM64 FortiGate

Dashboard

Status

Security

Network

Users & Devices

+

FortiView Sources

FortiView Destinations

FortiView Applications

FortiView Web Sites

FortiView Policies

FortiView Sessions

+

Security Fabric

Network

System

Policy & Objects

+ Add Widget

System Information

Hostname	FortiGate
Serial Number	FGVMEVL1KCWJTV
Firmware	v6.4.3 build1778 (GA)
Mode	NAT
System Time	2020/11/08 17:34:48
Uptime	00:00:20:23
WAN IP	Unknown

Security Fabric

Dashboard: – The dashboard displays various widgets that display important system information and allow you to configure some system options.

Security Fabric: – Access the physical topology, logical topology, audit, and settings of the Fortinet Security Fabric.

FortiView: – A collection of dashboards and logs that give insight into network traffic, showing which users are creating the most traffic, what sort of traffic it is, when the traffic occurs, and what kind of threat the traffic may pose to the network.

Network: – Options for networking, including configuring system interfaces and routing options.

System: – Configure system settings, such as administrators, FortiGuard, and certificates.

Policy & Objects: – Configure firewall policies, protocol options, and supporting content for policies, including schedules, firewall addresses, and traffic shapers.

Security Profiles: – Configure your FortiGate's security features, including Antivirus, Web Filter, and Application Control.

VPN: – Configure options for IPsec and SSL virtual private networks (VPNs).

User & Device: – Configure user accounts, groups, and authentication methods, including external authentication and single sign-on (SSO).

WiFi & Switch Controller: – Configure the unit to act as a wireless network controller, managing the wireless Access Point (AP) functionality of FortiWiFi and FortiAP units. On certain FortiGate models, this menu has additional features allowing for FortiSwitch units to be managed by the FortiGate.

Log & Report: – Configure logging and alert email as well as reports.

Monitor: – View a variety of monitors, including the Routing Monitor, VPN monitors for both IPsec and SSL, monitors relating to wireless networking, and more.

Dashboard Demonstration

FortiGate dashboards can have a Network Operations Centre (NOC) or responsive layout.

- On a responsive dashboard, the number of columns is determined by the size of the screen. Widgets can only be resized horizontally, but the dashboard will fit on all screen sizes.
- On a NOC dashboard, the number of columns is explicitly set. Widgets can be resized both vertically and horizontally, but the dashboard will look best on the screen size that it is configured for.

Multiple dashboards of both types can be created, for both individual VDOMs and globally.

- Widgets are interactive; clicking or hovering over most widgets shows additional information or links to relevant pages.
- Widgets can be reorganized by clicking and dragging them around the screen.

Four dashboards are available by default: Status, Network, Security, and System Events

The Status dashboard includes the following widgets by default:

System Information: – The System Information widget lists information relevant to the FortiGate system, including hostname, serial number, and firmware. Clicking on the widget provides links to configure system settings and update the device firmware.

Licenses: – The License widget lists the status of various licenses, such as FortiCare Support and IPS. The number of used and available FortiTokens is also shown. Clicking on the widget provides a link to the FortiGuard settings page.

Virtual Machine: – The VM widget (shown by default in the dashboard of a FortiOS VM device) includes:

- License status and type
- vCPU allocation and usage
- RAM allocation and usage
- VMX license information (if the VM supports VMX)

Clicking on an item in the widget provides a link to the FortiGate VM License page, where license files can be uploaded.

FortiGate Cloud: – This widget displays the FortiGate Cloud and FortiSandbox Cloud status.

Security Fabric: – The Security Fabric widget displays a visual summary of the devices in the Fortinet Security Fabric.

Clicking on a product icon provides a link to a page relevancy to that product. For example, clicking the FortiAnalyzer shows a link to log settings.

Security Rating: – The Security Rating widget shows the security rating for your Security Fabric. It can show the current rating percentile, or historical security rating score or percentile charts.

Administrators: – This widget allows you to see logged-in administrators, connected administrators, and the protocols used by each. Clicking in the widget provides links to view active administrator sessions, and to open the FortiExplorer page on the App Store.

CPU: – This widget shows real-time CPU usage over the selected time frame. Hovering over any point on the graph displays the percentage of CPU power used at that specific time. It can be expanded to occupy the entire dashboard.

Memory: – This widget shows real-time memory usage over the selected time frame. Hovering over any point on the graph displays the percentage of the memory used at that specific time. It can be expanded to occupy the entire dashboard.

Sessions: – This widget shows the current number of sessions over the selected time frame. Hovering over any point on the graph displays the number of sessions at that specific time. It can be expanded to occupy the entire dashboard.

The Security dashboard includes the following widgets by default:

- **Top Compromised Hosts by Verdict:** – This widget lists the compromised hosts by verdict. A FortiAnalyzer is required. It can be expanded to occupy the entire dashboard.
- **Top Threats by Threat Level:** – This widget lists the top threats by threat level, from FortiView. It can be expanded to occupy the entire dashboard.
- **FortiClient Detected Vulnerabilities:** – This widget shows the number of vulnerabilities detected by FortiClient. FortiClient must be enabled. Clicking on the widget provides a link to view the information in FortiView.

- **Host Scan Summary:** – This widget lists the total number of hosts. Clicking on the widget provides links to view vulnerable devices in FortiView, FortiClient monitor, and the device inventory.
- **Top Vulnerable Endpoint Devices by Detected Vulnerabilities:** – This widget lists the top vulnerable endpoints by the detected vulnerabilities, from FortiView. It can be expanded to occupy the entire dashboard.

The System Events dashboard includes the following widgets by default:

- **Top System Events by Events:** – This widget lists the top system events, sorted by the number of events. It can be expanded to occupy the entire dashboard. Double click on an event to view the specific event log.
- **Top System Events by Level:** – This widget lists the top system events, sorted by the events' levels. It can be expanded to occupy the entire dashboard. Double click on an event to view the specific event log.