

# **Application Security**

Day1

Nada Mohamed Ahmed Hassan Eleshmawy

Mansoura Open Source

Date : 6/4/2025

Download FG images from

[https://drive.google.com/drive/folders/16xkwICwgYpkdHj\\_g66eeSZHIMFJfl-8r?usp=drive\\_link](https://drive.google.com/drive/folders/16xkwICwgYpkdHj_g66eeSZHIMFJfl-8r?usp=drive_link)

1-Use VMWare workstation, Linux Virtual Machine (Web Server), Fortigate FW (FG Image)

2-Internal Virtual Network

1-In VMWare workstation, create a virtual switch

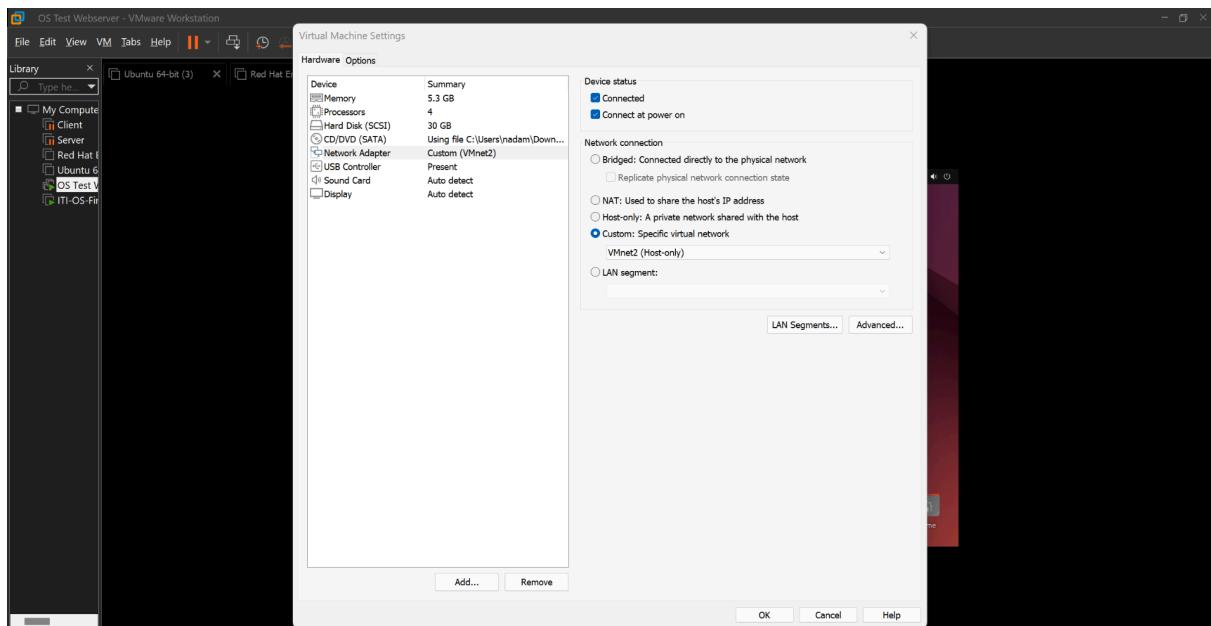
- 1-Open VMWare workstation
- 2>Edit/Virtual Network Editor
- 3-Add Network
- 4-Choose Host-only
- 5-Press Add
- 6-Press on VMNet0 (Bridged)
- 7-Bridged to: (Network interface connected to internet)
- 8-Press Save

2-In VMWare workstation, Create a Virtual Machine (Linux Web Server)

3-Configure VM Network

- 1-Right click on VM, choose settings
- 2-From left, choose network adapter
- 3-From right, choose Custom,\
- 4-Choose VMNet created in step 2-1-3
- 5-Choose save

4-Poweron VM

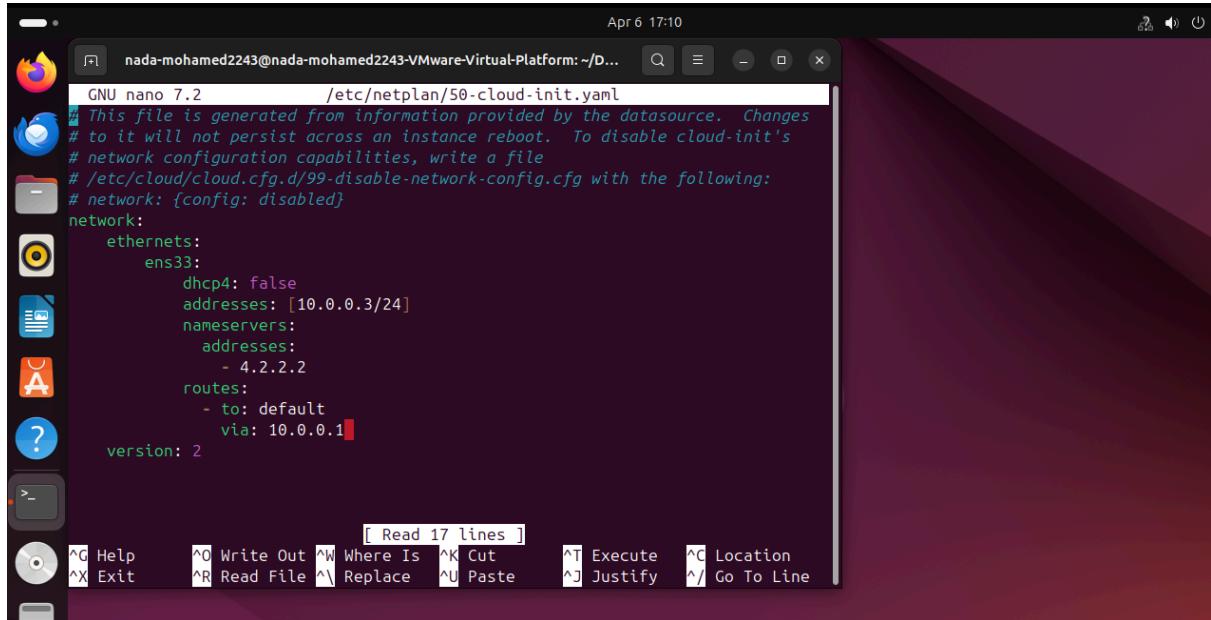


5-Configure VM Networking

1-Edit /etc/netplan/00-installer-config.yaml (don't find so i write here →  
**/etc/netplan/00-installer-config.yaml**)

2-dhcp4: true -> false

### 3-Save, exit, sudo netplan apply



```
GNU nano 7.2          /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}

network:
  ethernets:
    ens33:
      dhcp4: false
      addresses: [10.0.0.3/24]
      nameservers:
        addresses:
          - 4.2.2.2
      routes:
        - to: default
          via: 10.0.0.1
version: 2
```

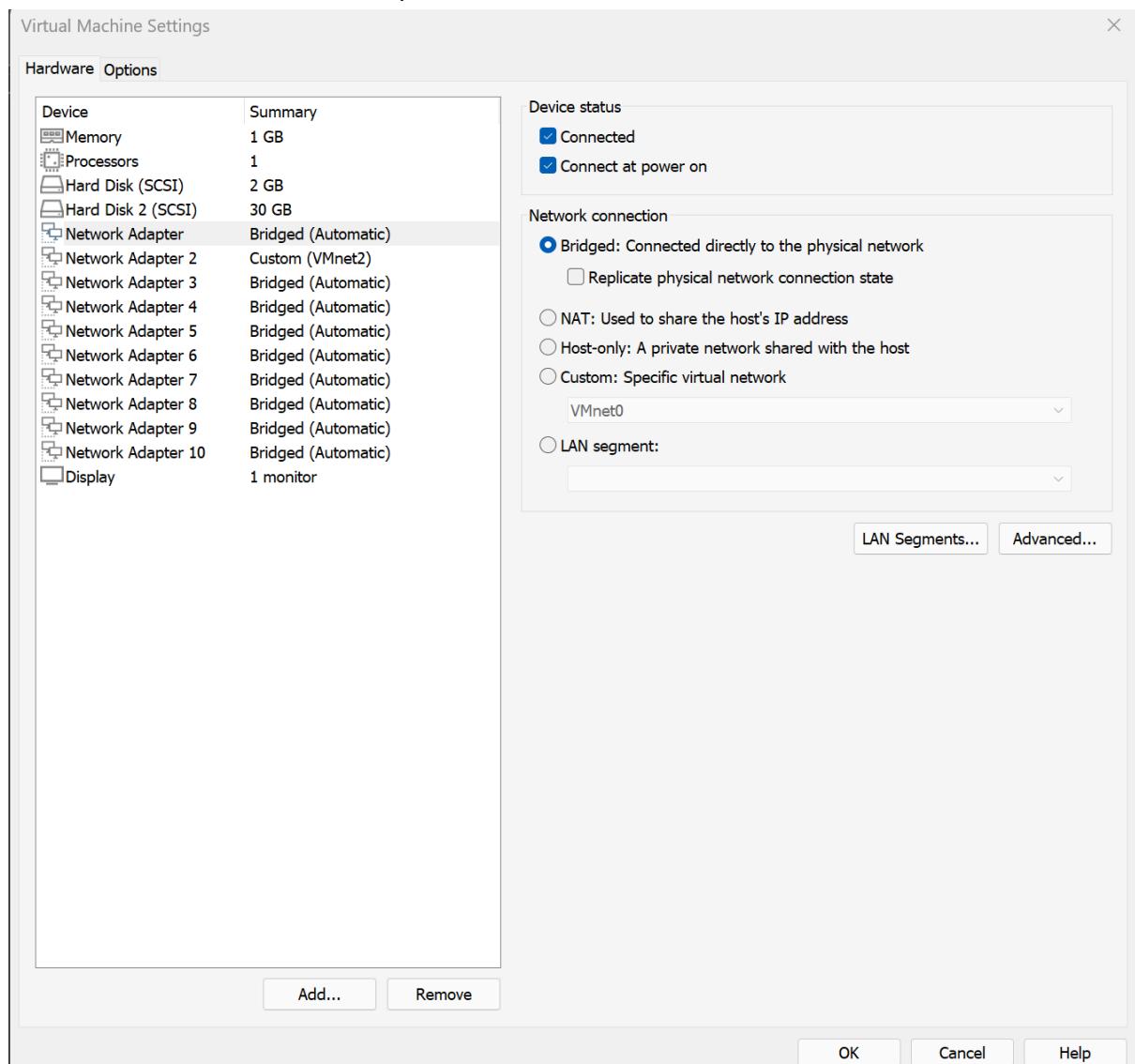
### 6-Create FortiGate VM

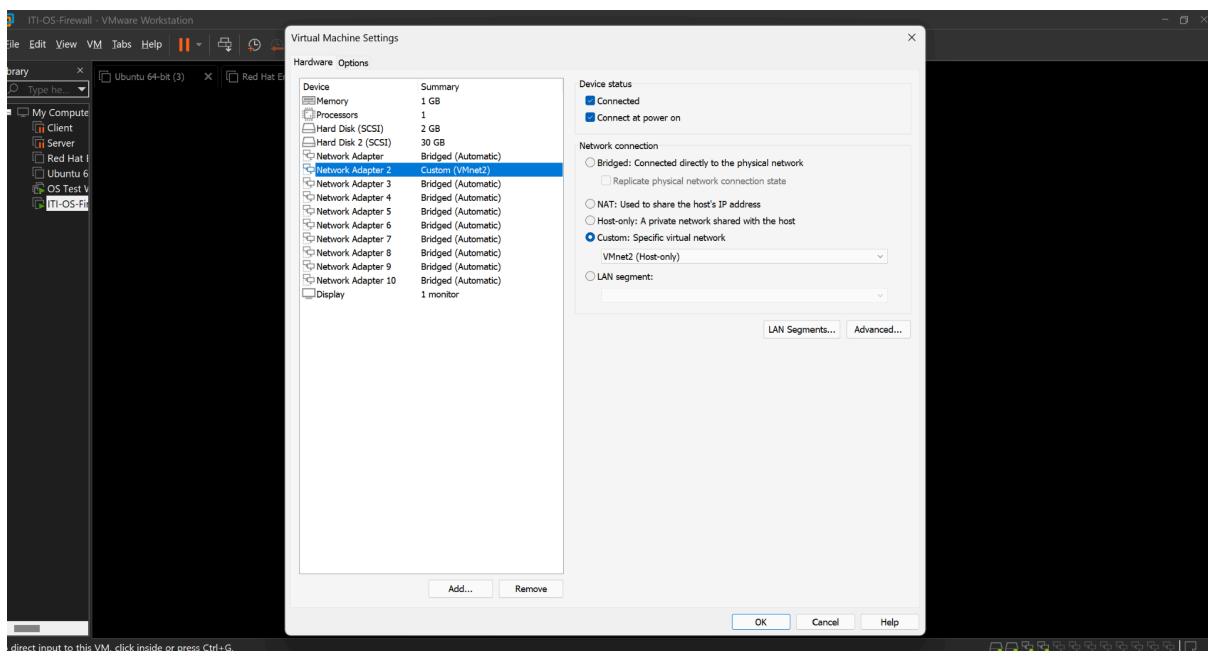
- 1-In VMWare workstation, press File/New
- 2-Locate Fortigate-VM64-hw07-vmxnet03.ovb
- 3-Check i Accept, press Next
- 4-Choose directory to store the VM
- 5-Press import
- 7-Right click on Firewall, PResst settings, clear all connect on poweron Interfaces
- 8-Choose Network ADAPTER 2: Change cutom to (VMNet4) the same as Web server
- 9-PResst save
- 10-Power on Fortigate FW
- 11-Login username admin, password blank no password
- 12-Configure Firewall management IP
  - 13-configure system interface
  - 14-edit port1
  - 15-set mode static
  - 16-set ip 192.168.1.100/24
  - 17-end
- 18-Configure firewall ntp (Disable)
  - 19-configure system ntp
  - 20-sety type custom
  - 21-set server-mode disable
  - 22-set ntpsync disable
  - 23-end
- 24-Reboot
- 25-execute reboot

The terminal window displays the boot process of a Linux distribution. The logs show:

```
Loading flatfs... ok
Loading /rootfs.gz...ok
Decompressing Linux... Parsing ELF... done.
Booting the kernel...
System is starting...
Starting local maintenance...
Scanning /dev/sda1... (BBB)
Scanning /dev/sda2... (BBB)
Serial number is F040000000000000
Port100-E064 login:
```

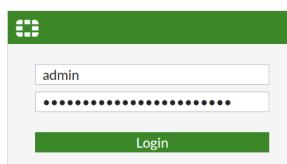
## 26-Connect Network adapter 1, and 2





## 27-Open your browser

<http://192.168.1.100>



The screenshot shows the FortiGate VM64 management console dashboard. The left sidebar includes sections like Dashboard, Status, Security Fabric, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, Log & Report, and Monitor. The main area displays System Information (Hostname: FortiGate-VM64, Serial Number: FGMEVWH7ZMJL79, Firmware: v6.2.4 build1112 (GA), Mode: NAT, System Time: 2025/04/06 10:06:11, Uptime: 00:00:15:7, WAN IP: Unknown), Licenses (FortiCare Support, Firmware & General Updates, IPS, AntiVirus, Web Filtering, FortiToken 0/0), Virtual Machine (FGMVE License, Allocated vCPUs 1/1, 100%, Allocated RAM 1000 MiB / 2 GiB, 49%), and Security Rating (disabled). A message at the bottom states "FortiGate Telemetry is disabled." The bottom right shows a refresh interval of 1 minute.

28-On FG management console, Press Network/Interfaces

29-Expand network list, Double click on port1.

Alias: ExternalPort

Role: WAN

Press OK

The screenshot shows the "Edit Interface" dialog for port1. The left sidebar under Network includes Interfaces, DNS, Packet Capture, SD-WAN, SD-WAN Rules, Performance SLA, Static Routes, Policy Routes, RIP, OSPF, BGP, Multicast, System, Policy & Objects, Security Profiles, VPN, and User & Device. The main dialog shows the following configuration:

- Name:** port1
- Alias:** External
- Type:** Physical Interface
- Role:** WAN
- Estimated bandwidth:** . kbps Upstream, . kbps Downstream
- Address:** Addressing mode: Manual, IP/Netmask: 192.168.1.100/255.255.255.0
- Administrative access:**
  - IPv4: HTTPS (checked), HTTP (checked), PING (checked), FMG-Access (unchecked), SSH (unchecked), RADIUS Accounting (unchecked), FTN (unchecked), SNMP (unchecked), Security Fabric Connection (unchecked)
  - Receive LLDP: Use VDOM Setting (Enable)
  - Transmit LLDP: Use VDOM Setting (Enable)
- Traffic Shaping:**

The right panel displays FortiGate information: Active Administrator Sessions (HTTP), Status (Up), MAC address (00:0c:29:0a:a0:56), and Documentation links (Online Help, Video Tutorials).

30-Double click on port2

Alias: ServerPort

Role: DMZ

IP/Network: 10.0.0.1/24

Administrative : Ping

**Edit Interface**

Name: port2  
Alias: Servers  
Type: Physical Interface  
Role: DMZ

Address  
Addressing mode: Manual  
IP/Netmask: 10.0.0.1/24  
Create address object matching subnet: Off  
Secondary IP address: Off

Administrative access  
IPv4: PING (checked), HTTPS, SSH, SNMP, RADIUS Accounting, Security Fabric Connection  
Receive LLDP: Use VDOM Setting (checked), Enable, Disable  
Transmit LLDP: Use VDOM Setting (checked), Enable, Disable

Network  
Device detection: Off

**FortiGate**  
FortiGate-VM64  
Status: Up  
MAC address: 00:0c:29:0:a:0:60  
Documentation, Online Help, Video Tutorials

**Interfaces**

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
External (port1)	Physical Interface		192.168.1.100/255.255.255.0	PING HTTPS HTTP	0		
port10	Physical Interface		0.0.0.0/0.0.0		0		
port3	Physical Interface		0.0.0.0/0.0.0		0		
port4	Physical Interface		0.0.0.0/0.0.0		0		
port5	Physical Interface		0.0.0.0/0.0.0		0		
port6	Physical Interface		0.0.0.0/0.0.0		0		
port7	Physical Interface		0.0.0.0/0.0.0		0		
port8	Physical Interface		0.0.0.0/0.0.0		0		
port9	Physical Interface		0.0.0.0/0.0.0		0		
Servers (port2)	Physical Interface		10.0.0.1/255.255.255.0	PING	0		

31-From VM:

ping 10.0.0.1 : Success

```
nada-mohamed2243@nada-mohamed2243-VMware-Virtual-Platform:~/Desktop$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=255 time=0.250 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=255 time=0.344 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=255 time=0.267 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=255 time=0.430 ms
64 bytes from 10.0.0.1: icmp_seq=5 ttl=255 time=0.508 ms
64 bytes from 10.0.0.1: icmp_seq=6 ttl=255 time=0.648 ms
64 bytes from 10.0.0.1: icmp_seq=7 ttl=255 time=0.458 ms
64 bytes from 10.0.0.1: icmp_seq=8 ttl=255 time=0.626 ms
64 bytes from 10.0.0.1: icmp_seq=9 ttl=255 time=0.431 ms
64 bytes from 10.0.0.1: icmp_seq=10 ttl=255 time=0.417 ms
64 bytes from 10.0.0.1: icmp_seq=11 ttl=255 time=0.215 ms
64 bytes from 10.0.0.1: icmp_seq=12 ttl=255 time=0.422 ms
64 bytes from 10.0.0.1: icmp_seq=13 ttl=255 time=0.419 ms
64 bytes from 10.0.0.1: icmp_seq=14 ttl=255 time=0.422 ms
64 bytes from 10.0.0.1: icmp_seq=15 ttl=255 time=0.547 ms
64 bytes from 10.0.0.1: icmp_seq=16 ttl=255 time=0.434 ms
64 bytes from 10.0.0.1: icmp_seq=17 ttl=255 time=0.477 ms
64 bytes from 10.0.0.1: icmp_seq=18 ttl=255 time=0.423 ms
64 bytes from 10.0.0.1: icmp_seq=19 ttl=255 time=0.463 ms
64 bytes from 10.0.0.1: icmp_seq=20 ttl=255 time=0.460 ms
64 bytes from 10.0.0.1: icmp_seq=21 ttl=255 time=0.437 ms
64 bytes from 10.0.0.1: icmp_seq=22 ttl=255 time=0.383 ms
64 bytes from 10.0.0.1: icmp_seq=23 ttl=255 time=0.444 ms
64 bytes from 10.0.0.1: icmp_seq=24 ttl=255 time=0.445 ms
64 bytes from 10.0.0.1: icmp_seq=25 ttl=255 time=0.495 ms
64 bytes from 10.0.0.1: icmp_seq=26 ttl=255 time=0.518 ms
64 bytes from 10.0.0.1: icmp_seq=27 ttl=255 time=0.389 ms
64 bytes from 10.0.0.1: icmp_seq=28 ttl=255 time=0.449 ms
64 bytes from 10.0.0.1: icmp_seq=29 ttl=255 time=0.426 ms
64 bytes from 10.0.0.1: icmp_seq=30 ttl=255 time=0.459 ms
64 bytes from 10.0.0.1: icmp_seq=31 ttl=255 time=0.422 ms
```

ping 4.2.2.2 : Not (FG can not access internet, no policy enable VM to access internet)

```
nada-mohamed2243@nada-mohamed2243-VMware-Virtual-Platform:~/Desktop$ ping 4.2.2.2
PING 4.2.2.2 (4.2.2.2) 56(84) bytes of data.
From 10.0.0.1 icmp_seq=2 Destination Net Unreachable
From 10.0.0.1 icmp_seq=4 Destination Net Unreachable
From 10.0.0.1 icmp_seq=5 Destination Net Unreachable
From 10.0.0.1 icmp_seq=9 Destination Net Unreachable
From 10.0.0.1 icmp_seq=10 Destination Net Unreachable
From 10.0.0.1 icmp_seq=11 Destination Net Unreachable
From 10.0.0.1 icmp_seq=12 Destination Net Unreachable
From 10.0.0.1 icmp_seq=17 Destination Net Unreachable
From 10.0.0.1 icmp_seq=19 Destination Net Unreachable
From 10.0.0.1 icmp_seq=20 Destination Net Unreachable
From 10.0.0.1 icmp_seq=24 Destination Net Unreachable
From 10.0.0.1 icmp_seq=25 Destination Net Unreachable
From 10.0.0.1 icmp_seq=26 Destination Net Unreachable
From 10.0.0.1 icmp_seq=27 Destination Net Unreachable
From 10.0.0.1 icmp_seq=28 Destination Net Unreachable
From 10.0.0.1 icmp_seq=29 Destination Net Unreachable
From 10.0.0.1 icmp_seq=33 Destination Net Unreachable
From 10.0.0.1 icmp_seq=34 Destination Net Unreachable
```

### 31-Test Fortigate connection to internet

From FG command line, execute ping 4.2.2.2

```

Serial number is FGUMEVLWH72MJL79

FortiGate-VM64 login: admin
Password: *****
Welcome !

WARNING: File System Check Recommended! Unsafe reboot may have caused inconsistency in disk drive.
It is strongly recommended that you check file system consistency before proceeding.
Please run the 'execute disk list' and then 'execute disk scan <ref#>'.
Note: The device will reboot and scan during startup. This may take up to an hour.

FortiGate-VM64 # execute ping 4.2.2.2
PING 4.2.2.2 (4.2.2.2): 56 data bytes
sendto failed
sendto failed
sendto failed
sendto failed
sendto failed

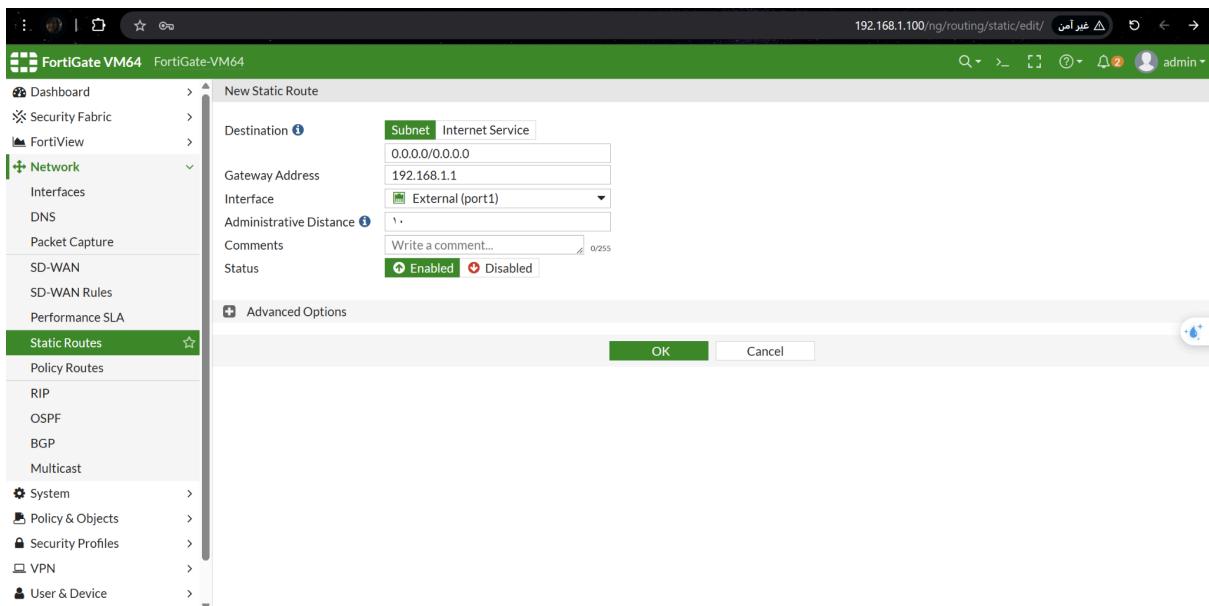
--- 4.2.2.2 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss

FortiGate-VM64 #

```

FG can not ping internet (Because FG has no Default route)

32-To configure FG Default route (Network/Static routes), Press create new, gateway : 192.168.1.1,interface port1, press ok



-Test Fortigate connection to internet again

From FG command line, execute ping 4.2.2.2 (work successfully)

```

FortiGate-VM64 # execute ping 4.2.2.2
PING 4.2.2.2 (4.2.2.2): 56 data bytes
64 bytes from 4.2.2.2: icmp_seq=0 ttl=55 time=73.4 ms
64 bytes from 4.2.2.2: icmp_seq=1 ttl=55 time=73.3 ms
64 bytes from 4.2.2.2: icmp_seq=2 ttl=55 time=73.0 ms
64 bytes from 4.2.2.2: icmp_seq=3 ttl=55 time=74.2 ms
64 bytes from 4.2.2.2: icmp_seq=4 ttl=55 time=73.6 ms

--- 4.2.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 73.0/73.5/74.2 ms

FortiGate-VM64 #

```

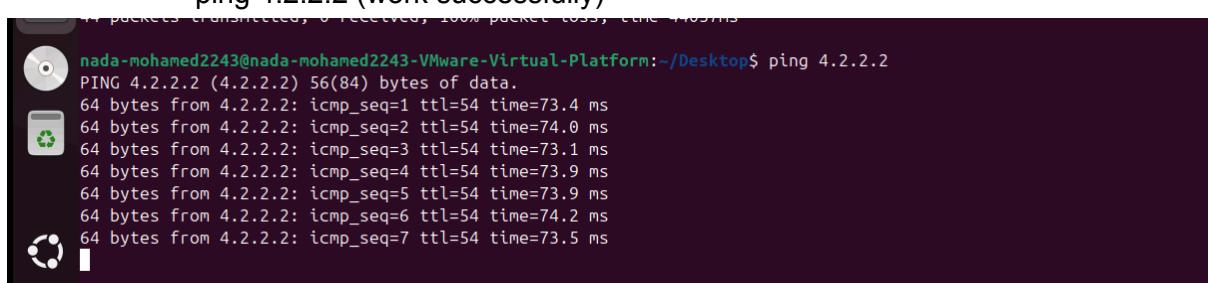
33-Create a FG policy to enable internet access to the VM

34-In FG console, Policy & Objects / IPv4 Policy/ Create new policy

Name: ServerToInternet

Now in VM : try again

- ping 4.2.2.2 (work successfully)



- sudo apt update

```
nada-mohamed2243@nada-mohamed2243-VMware-Virtual-Platform:~/Desktop$ sudo apt update
[sudo] password for nada-mohamed2243:
Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:2 http://eg.archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://eg.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [737 kB]
Get:5 http://eg.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:6 http://eg.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [987 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main i386 Packages [259 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [141 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [9,016 B]
Get:10 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [7,068 B]
Get:11 http://security.ubuntu.com/ubuntu noble-security/restricted i386 Packages [15.6 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [849 kB]
Get:13 http://eg.archive.ubuntu.com/ubuntu noble-updates/main i386 Packages [449 kB]
Get:14 http://eg.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [218 kB]
Get:15 http://eg.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [151 kB]
Get:16 http://eg.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [13.5 kB]
Get:17 http://eg.archive.ubuntu.com/ubuntu noble-updates/restricted i386 Packages [15.8 kB]
Get:18 http://eg.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [887 kB]
Get:19 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [172 kB]
Get:20 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:21 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 c-n-f Metadata [468 B]
Get:22 http://security.ubuntu.com/ubuntu noble-security/universe i386 Packages [513 kB]
Get:23 http://eg.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [180 kB]
Get:24 http://eg.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:25 http://eg.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 c-n-f Metadata [492 B]
Get:26 http://eg.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1,050 kB]
Get:27 http://eg.archive.ubuntu.com/ubuntu noble-security/universe amd64 Packages [828 kB]
Get:28 http://eg.archive.ubuntu.com/ubuntu noble-updates/universe i386 Packages [635 kB]
Get:29 http://eg.archive.ubuntu.com/ubuntu noble-security/universe Translation-en [190 kB]
```

## We have high traffic

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	ServerToInternet	all	all	always	ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled	SSL no-inspection	UTM	11.22 MB

```
nada-mohamed2243@nada-mohamed2243-VMware-Virtual-Platform:~/Desktop$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.58-1ubuntu8.5).
0 upgraded, 0 newly installed, 0 to remove and 352 not upgraded.
nada-mohamed2243@nada-mohamed2243-VMware-Virtual-Platform:~/Desktop$ sudo systemctl restart apache2
nada-mohamed2243@nada-mohamed2243-VMware-Virtual-Platform:~/Desktop$
```

You task for day1:

Need to open browser:

<http://192.168.1.100:8080> -> Web server 10.0.0.3 replies

Configure Fortigate to forward all incoming traffic to port 8080 to 10.0.0.3:80

## Step 1: Verify Current Configuration

First, confirm your FortiGate interfaces are properly set up:  
(we already do this)

- port1 (WAN): Should have 192.168.1.100/24 (connected to your main network)
- port2 (DMZ): Should have 10.0.0.1/24 (connected to web server)

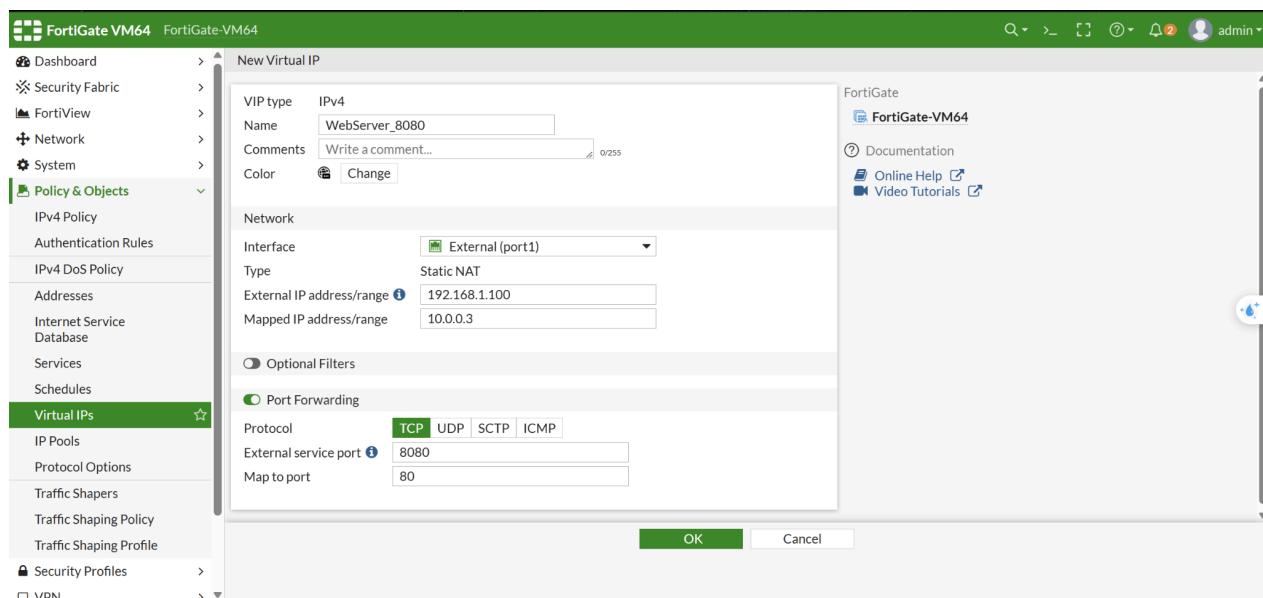
## Step 2: Configure Port Forwarding

1- Log in to FortiGate web interface (<https://192.168.1.100>)

2- Go to Policy & Objects → Virtual IPs

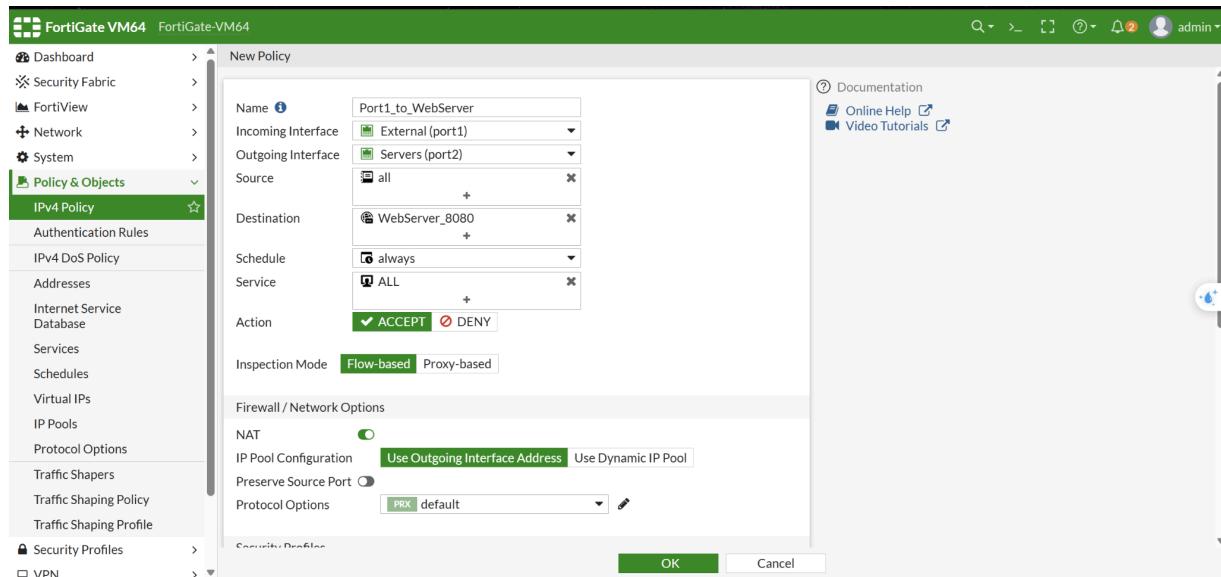
3- Click Create New → Virtual IP

- Name: WebServer\_8080
- Interface: port1
- External IP Address/Range: 192.168.1.100
- Mapped IP Address/Range: 10.0.0.3
- Port Forwarding: Enable
- External Service Port: 8080
- Map to Port: 80
- Click OK



## Step 3: Create Firewall Policy

1. Go to Policy & Objects → IPv4 Policy
2. Click Create New
  - Name: Port1\_to\_WebServer
  - Incoming Interface: port1
  - Outgoing Interface: port2
  - Source: all
  - Destination: WebServer\_8080 (the VIP we just created in step 2)
  - Service: ALL
  - Action: ACCEPT
  - Enable NAT
  - Click OK



ID	Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log	Bytes
1	External (port1) → Servers (port2)								
2	Port1_to_WebServer	all	WebServer_8080	always	ALL	✓ ACCEPT	Enabled	ssl no-inspection	0 B
3	Servers (port2) → External (port1)								
4	ServerToInternet	all	all	always	ALL	✓ ACCEPT	Enabled	ssl no-inspection	11.23 MB
5	Implicit								

## Step 4: Verify Configuration

### 1- Check if web server is running on 10.0.0.3:80 (from FortiGate CLI):

- execute ping 10.0.0.3

```
FortiGate-VM64 # execute ping 10.0.0.3
PING 10.0.0.3 (10.0.0.3): 56 data bytes
64 bytes from 10.0.0.3: icmp_seq=0 ttl=64 time=0.4 ms
64 bytes from 10.0.0.3: icmp_seq=1 ttl=64 time=0.4 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=64 time=1.1 ms
64 bytes from 10.0.0.3: icmp_seq=3 ttl=64 time=1.1 ms
64 bytes from 10.0.0.3: icmp_seq=4 ttl=64 time=0.9 ms

--- 10.0.0.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.7/1.1 ms
```

```
FortiGate-VM64 #
```

- telnet 10.0.0.3 80

```
FortiGate-VM64 # execute telnet 10.0.0.3 80
Trying 10.0.0.3...
Connected to 10.0.0.3.
```

### 2- Test port forwarding from your host machine:

- telnet 192.168.1.100 8080

```
nada-mohamed2243@nada-mohamed2243-VMware-Virtual-Platform:~/Desktop$ telnet 192.168.1.100 8080
Trying 192.168.1.100...
Connected to 192.168.1.100.
```

- or open in browser: http://192.168.1.100:8080

