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/16xkwlCwgYpkdHj_g66eeSZHlMFJfl-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

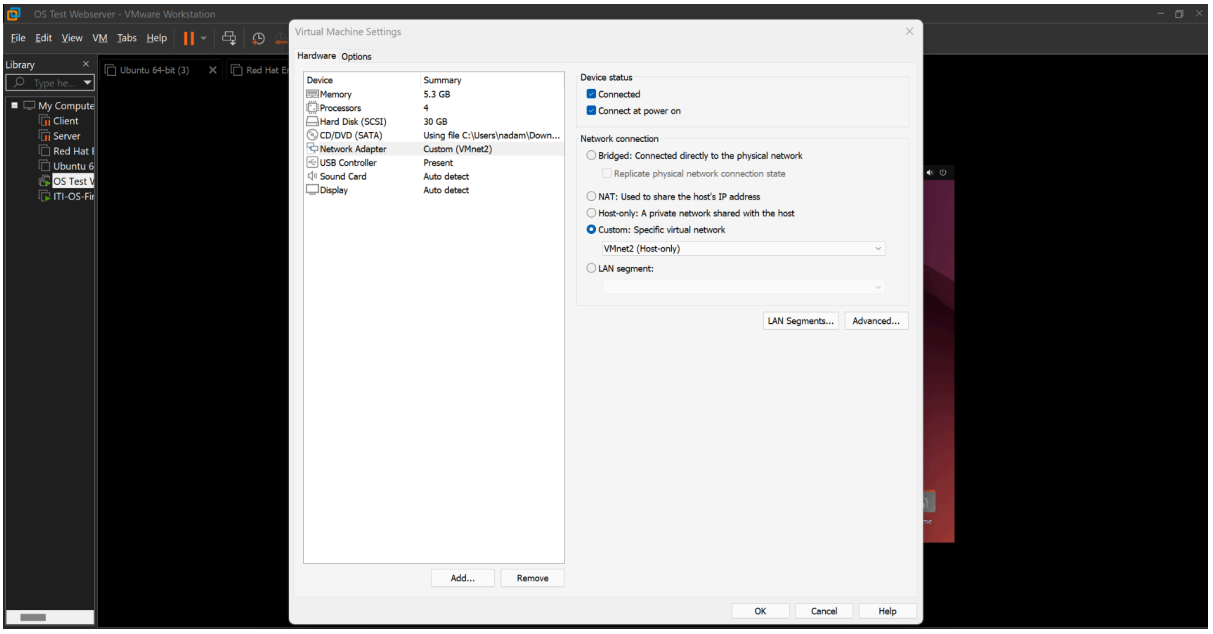
1-Open VMWare workstation
2-Edit/Virtual Network Editor
3-Add Network
4-Choose Host-only
5-Press Add
6-Press on VMNet0 (Bridged)
7-Bridged to: (Network interface connected to internet)
8-Press Save

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

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, PRess settings, clear all connect on poweron Interfaces

8-Choose Network ADapter 2: Change cutom to (VMNet4) the same as Web server

9-PRess 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

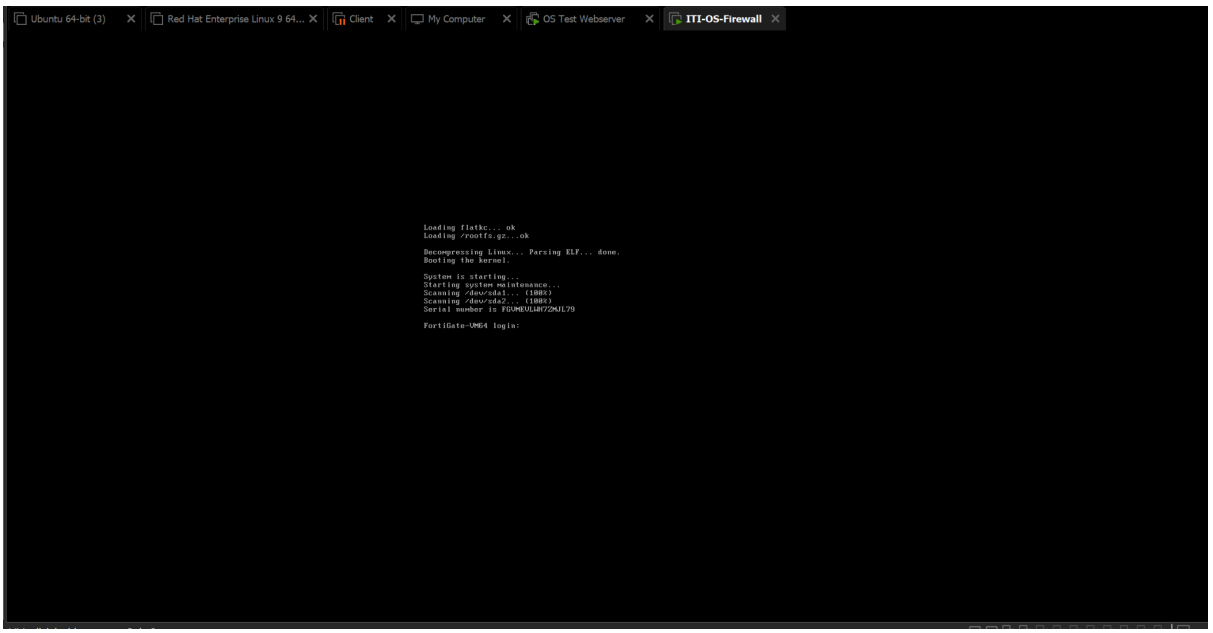
21-set server-mode disable

22-set ntpsync disable

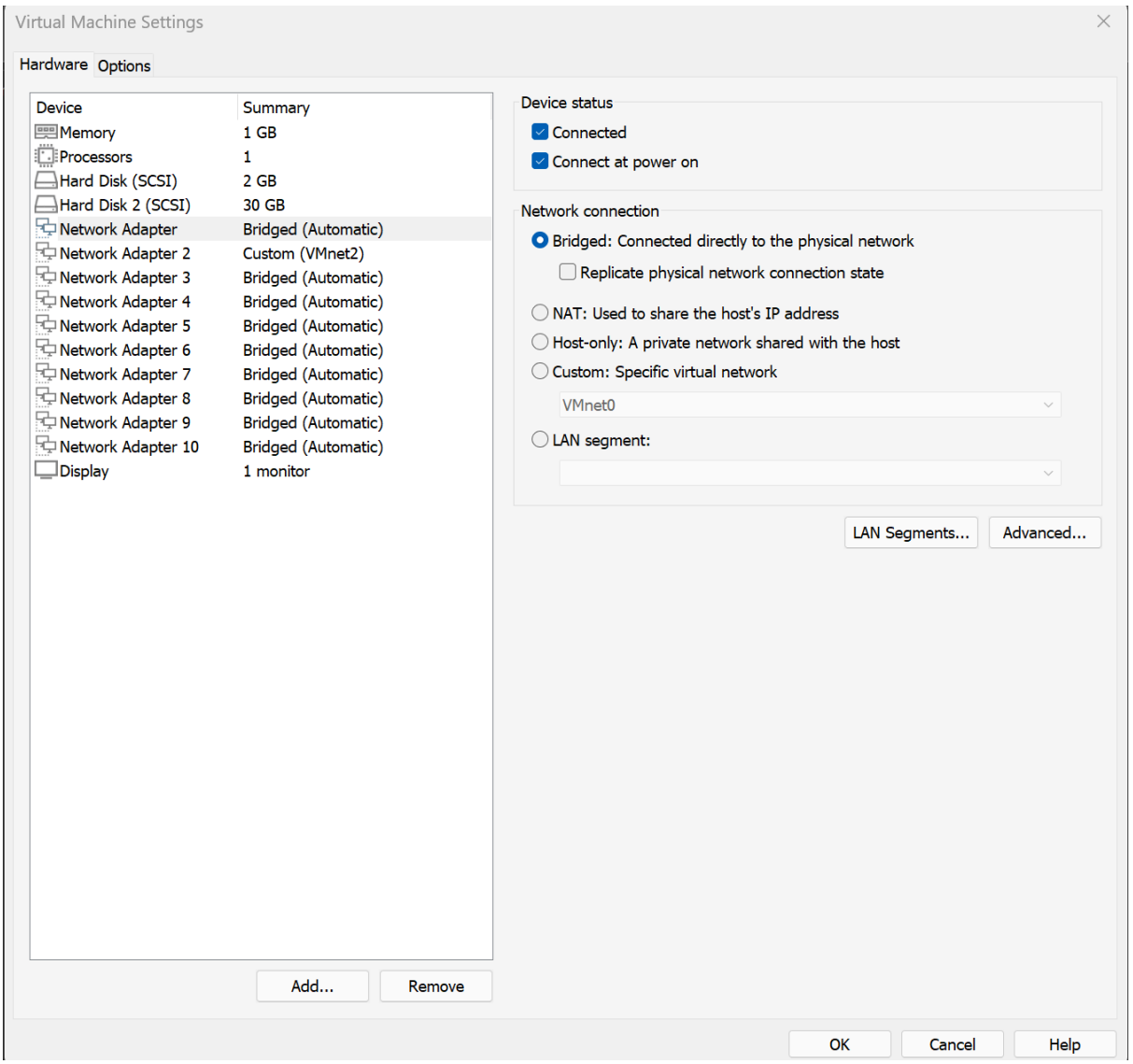
23-end

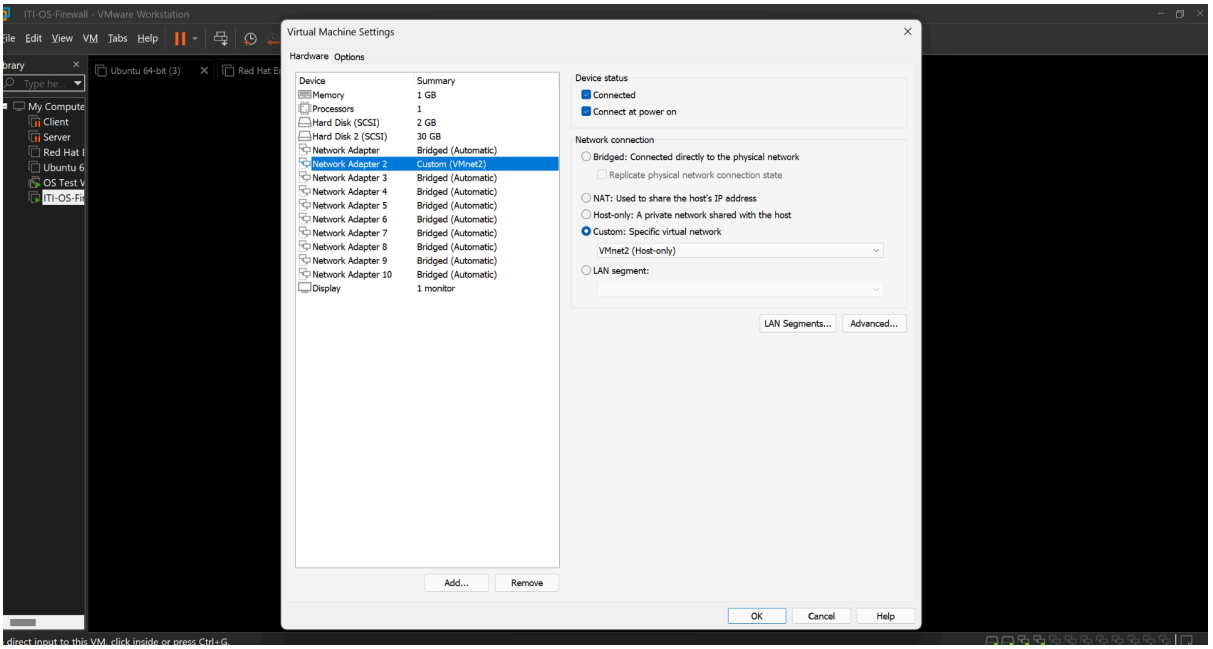
24-Reboot

25-execute reboot



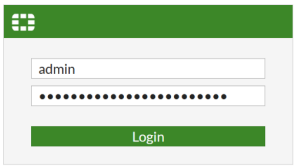
26-Connect Network adapter 1, and 2

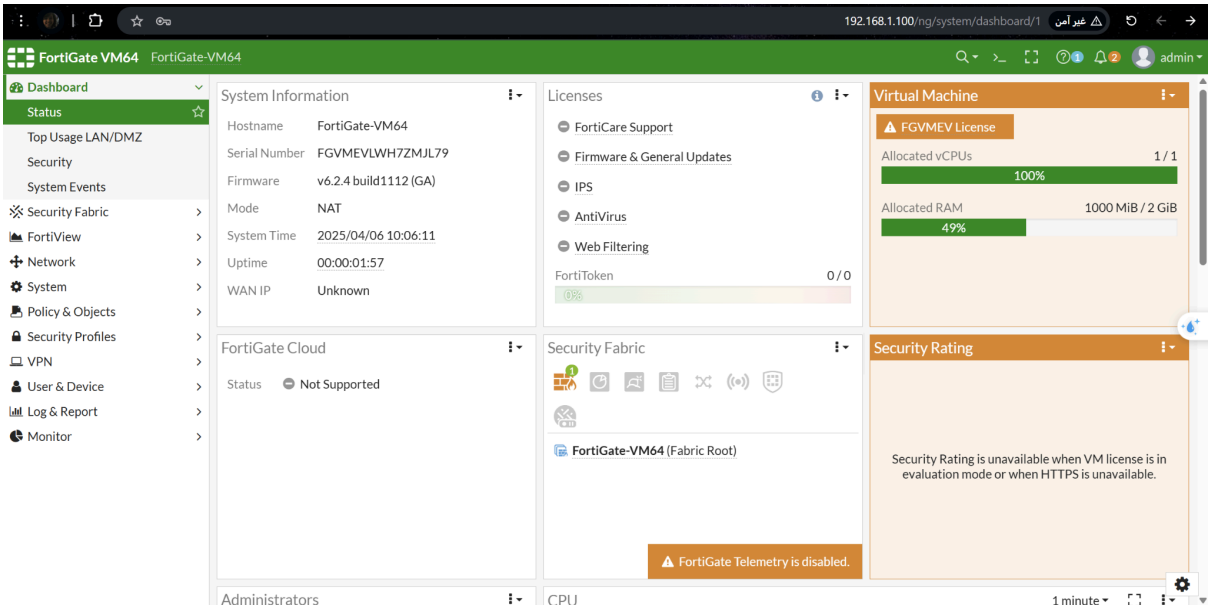




27-Open your browser

http://192.168.1.100





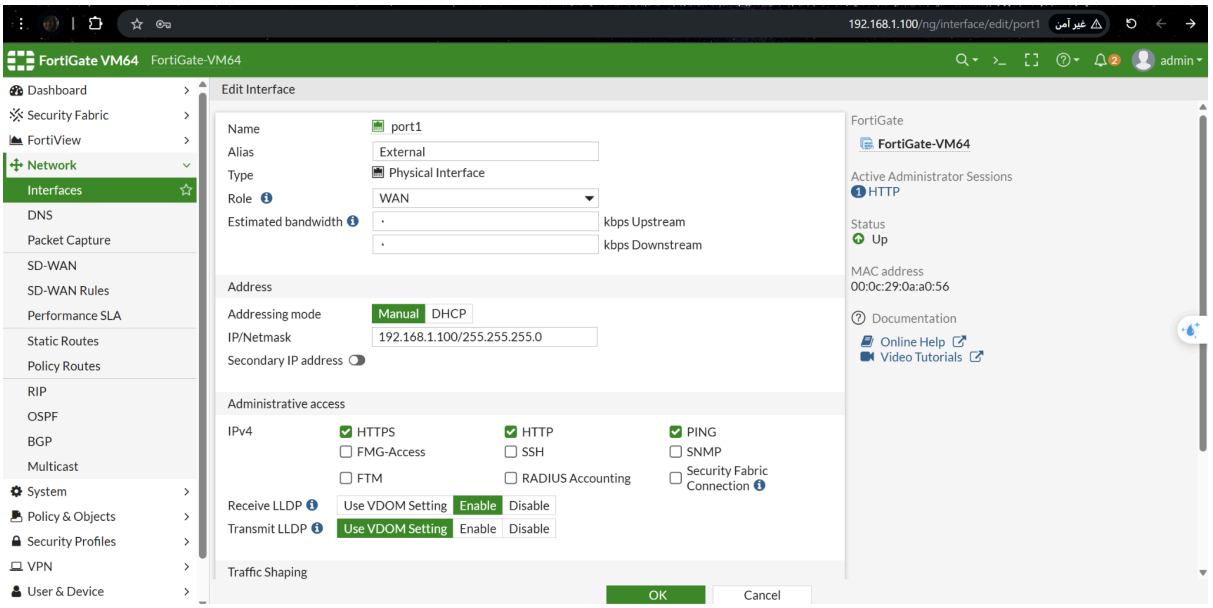
28-On FG management console, Press Network/Interfaces

29-Expand network list, Double click on port1.

Alias: ExternalPort

Role: WAN

Press OK



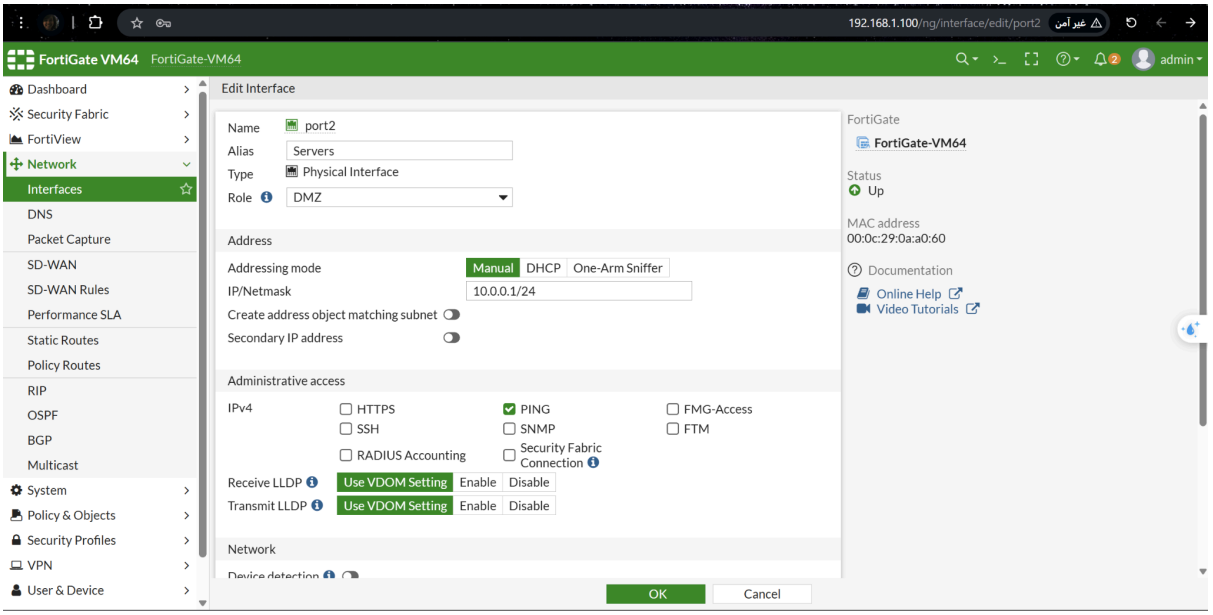
30-Double click on port2

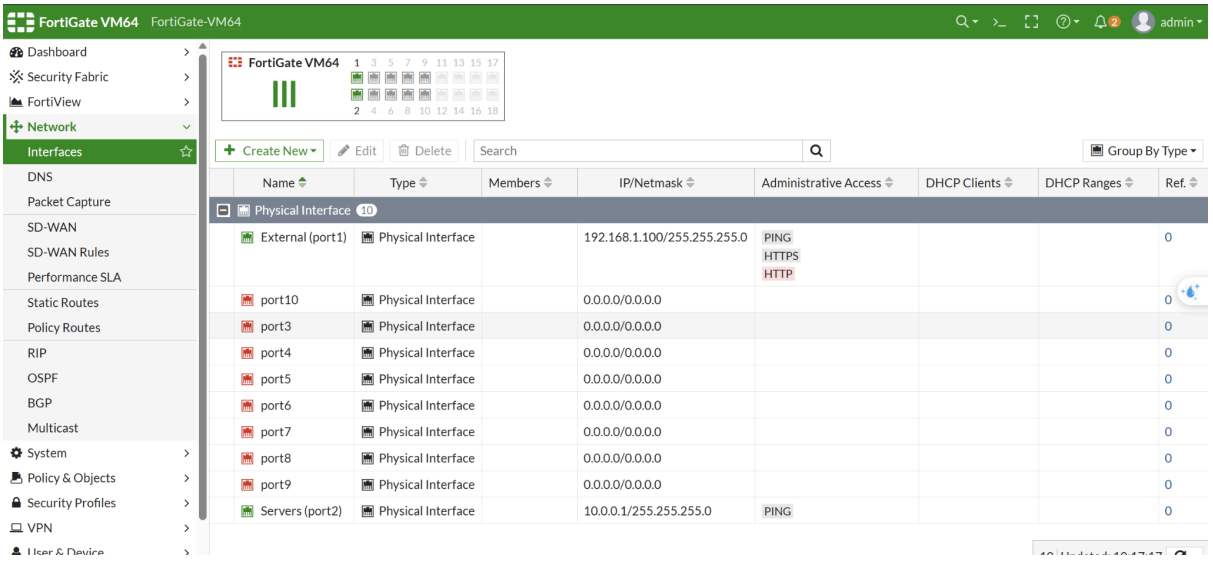
Alias: ServerPort

Role: DMZ

IP/Network: 10.0.0.1/24

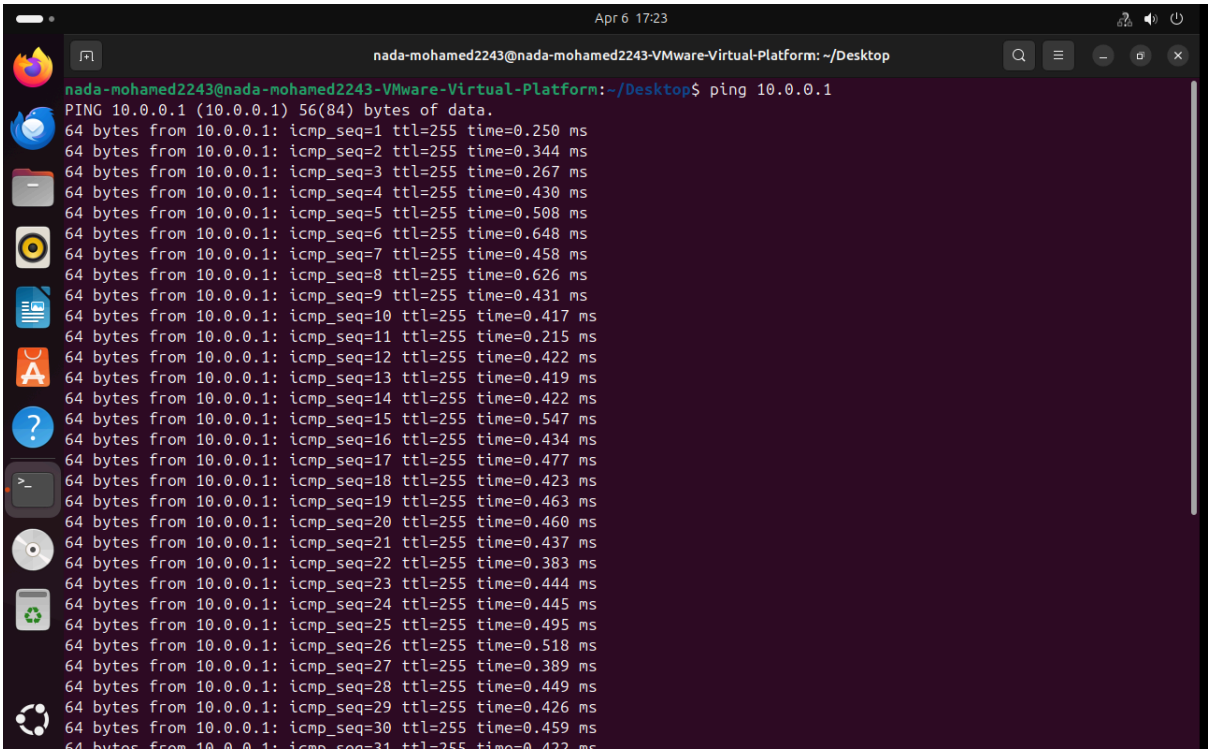
Administrative : Ping



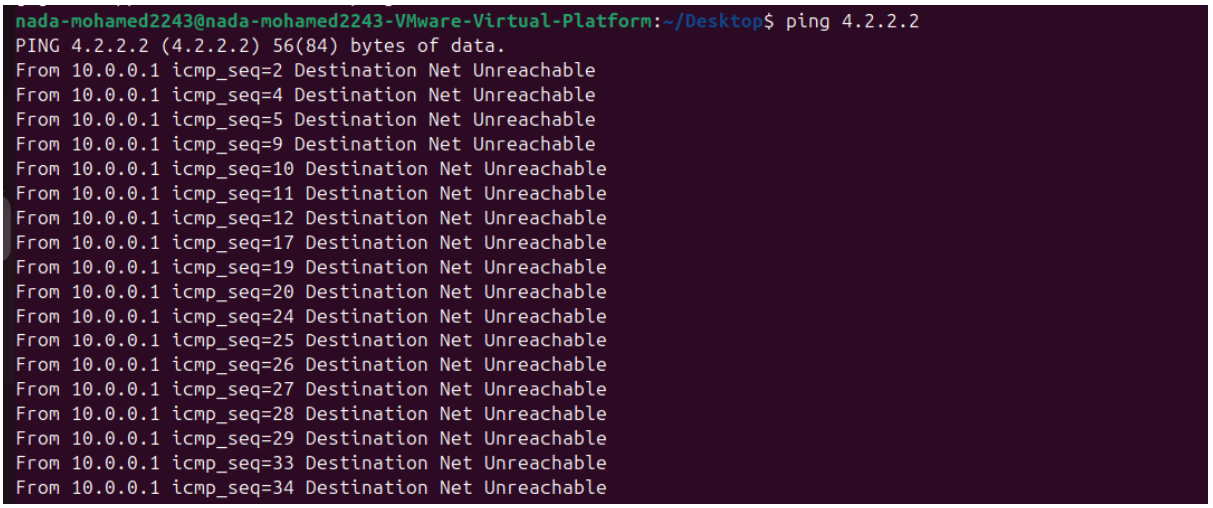


31-From VM:

ping 10.0.0.1 : Success



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



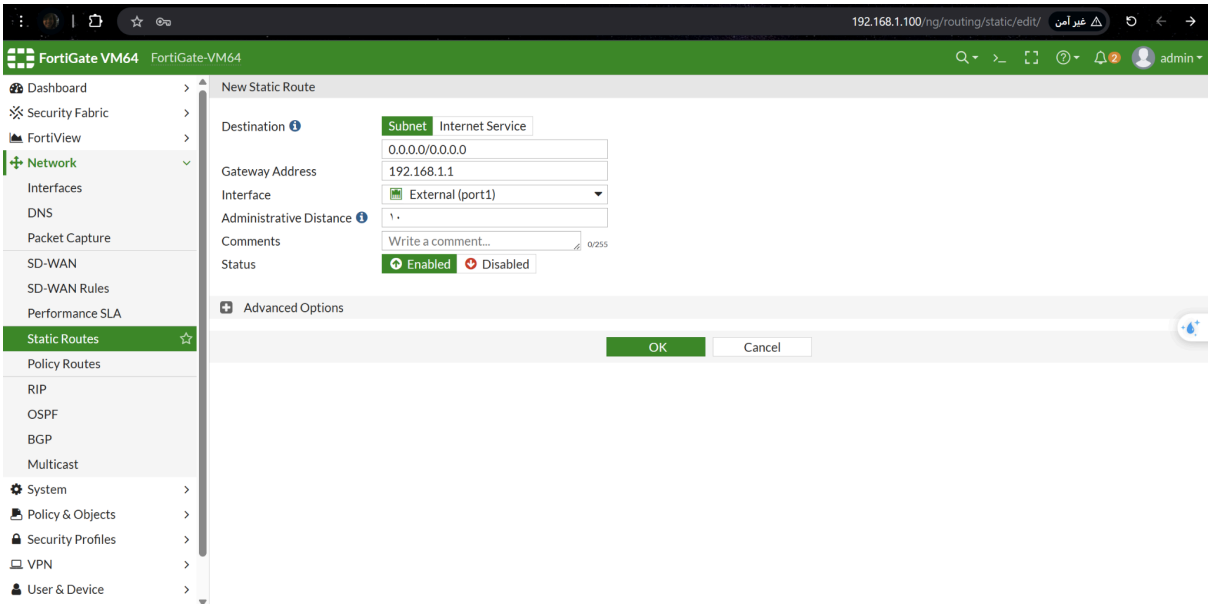
31-Test Fortigate connection to internet

From FG command line, execute ping 4.2.2.2

```
Serial number is FGVMEVLWH7ZMJL79

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

WARNING: File System Check Recommended! Unsafe reboot may have caused inconsiste
ncy in disk drive.
It is strongly recommended that you check file system consistency before proceed
ing.
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 hou
r
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

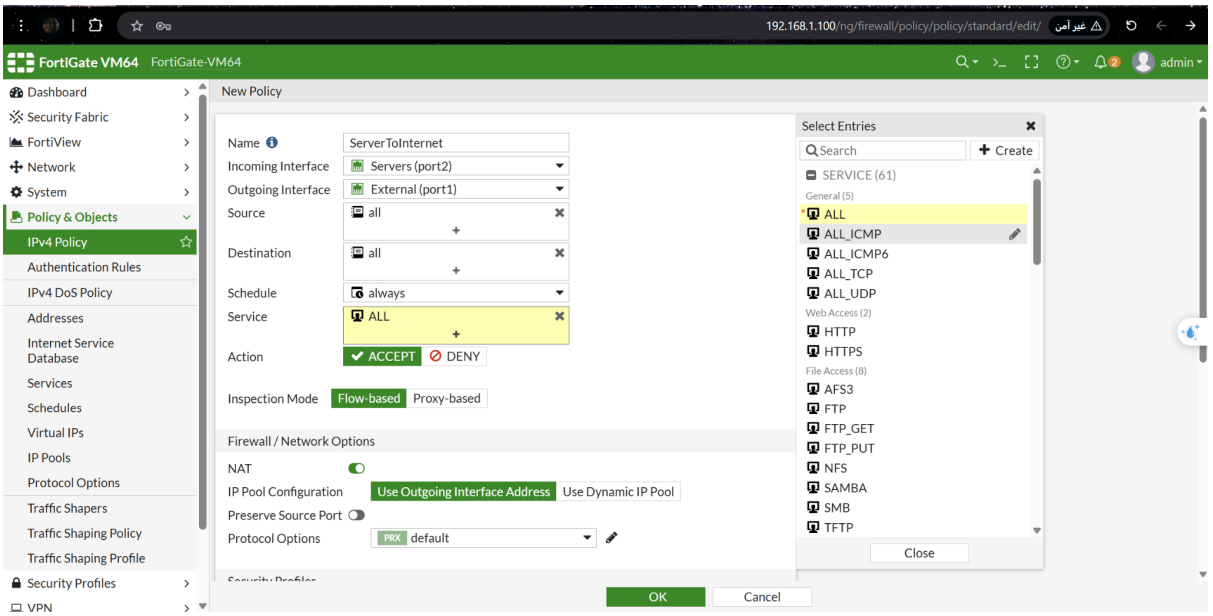
From FG command line, execute ping 4.2.2.2 (work successfully)

```
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

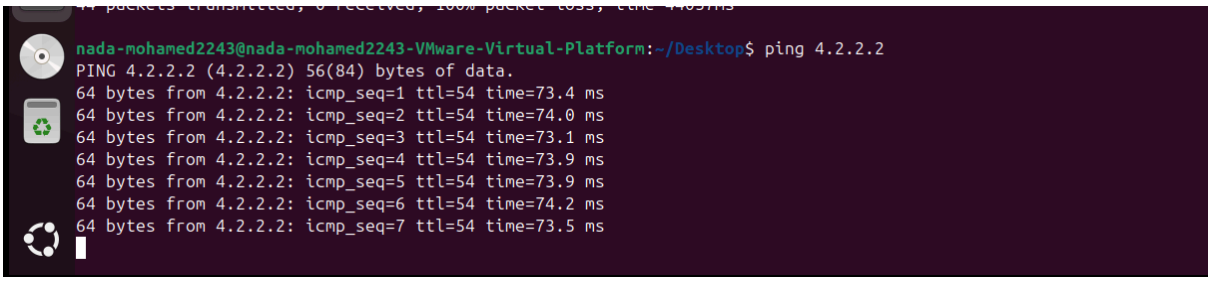
34-In FG console, Policy & Objects / IPv4 Policy/ Create new policy

Name: ServerToInternet



Now in VM : try again

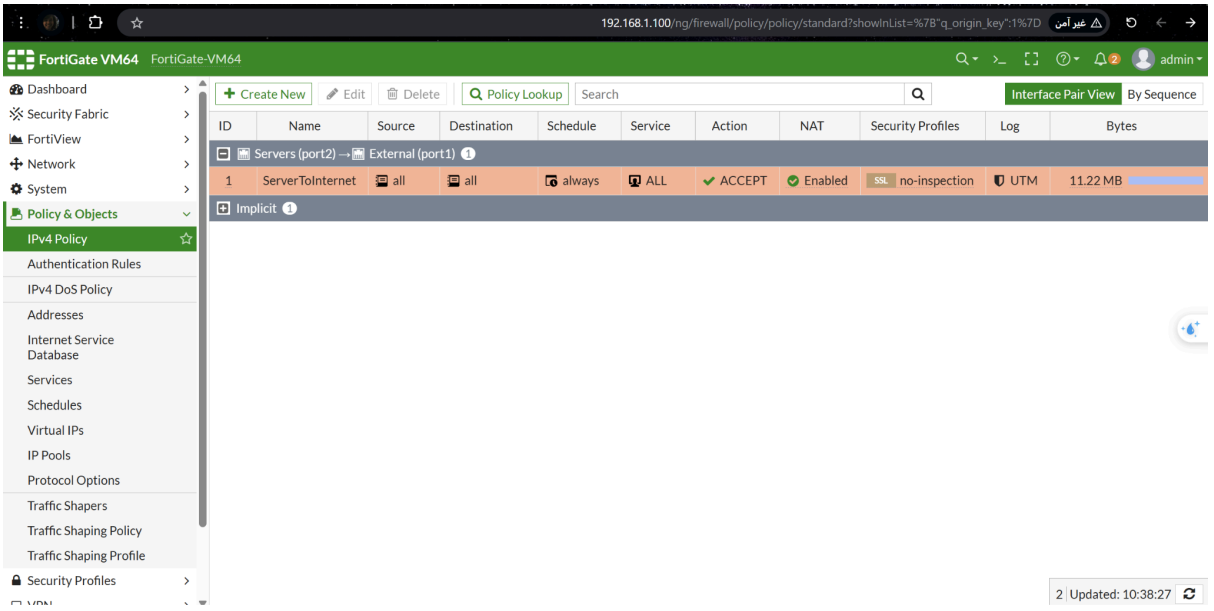
- ping 4.2.2.2 (work successfully)



- 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://security.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]
```

We have high traffic




```
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)

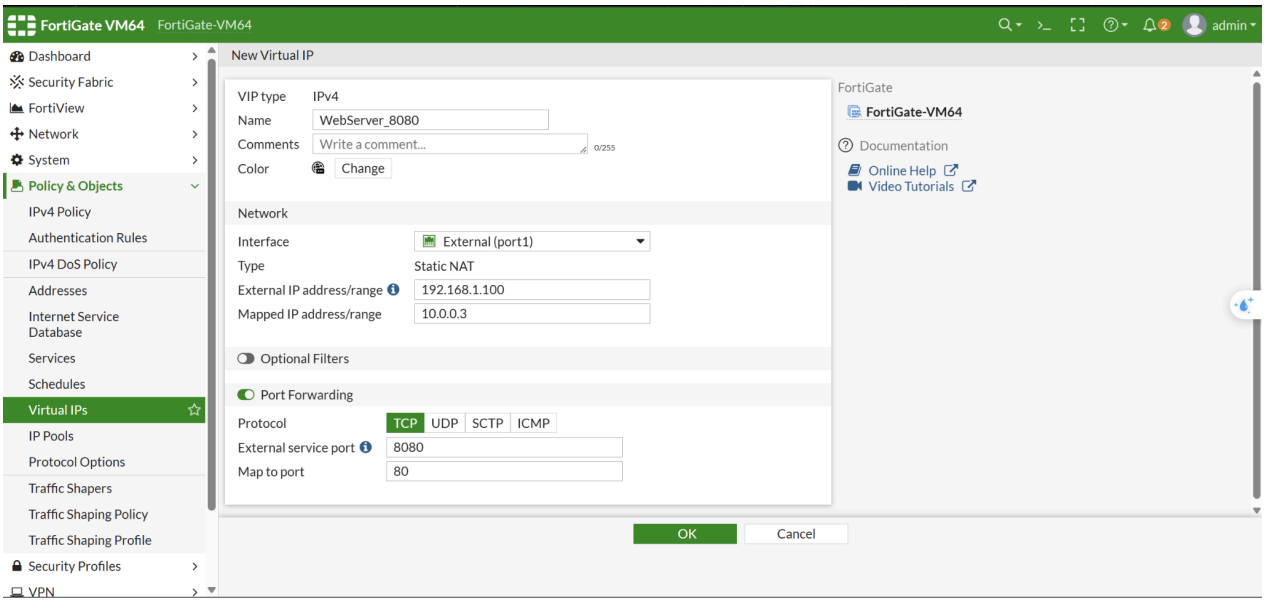
Step 2: Configure Port Forwarding

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

2- Go to Policy & Objects → Virtual IPs

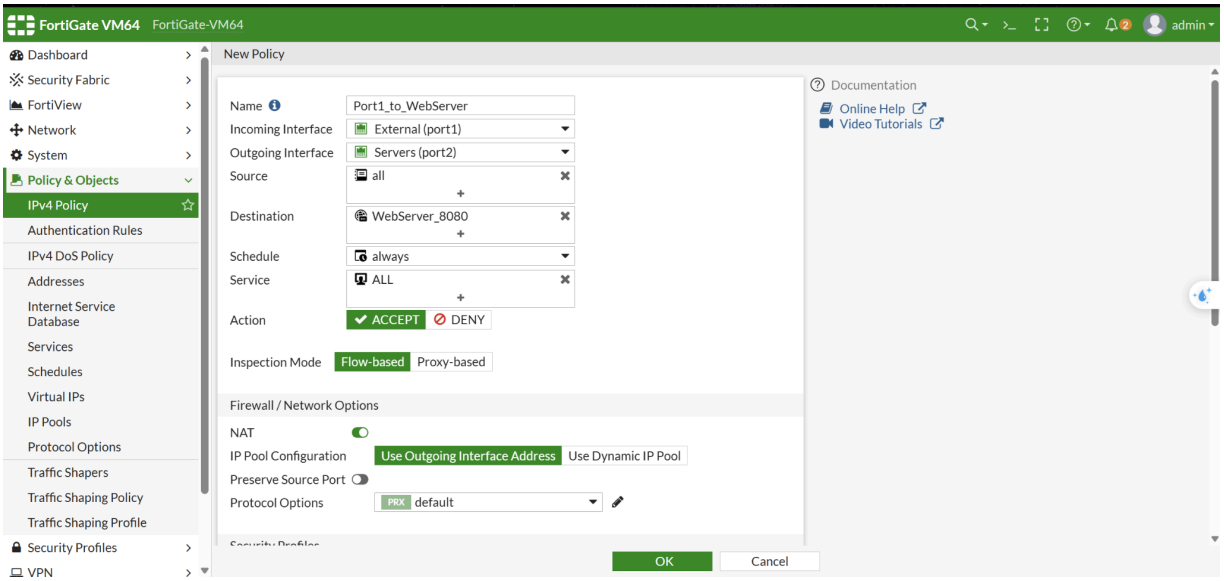
3- Click Create New → Virtual IP

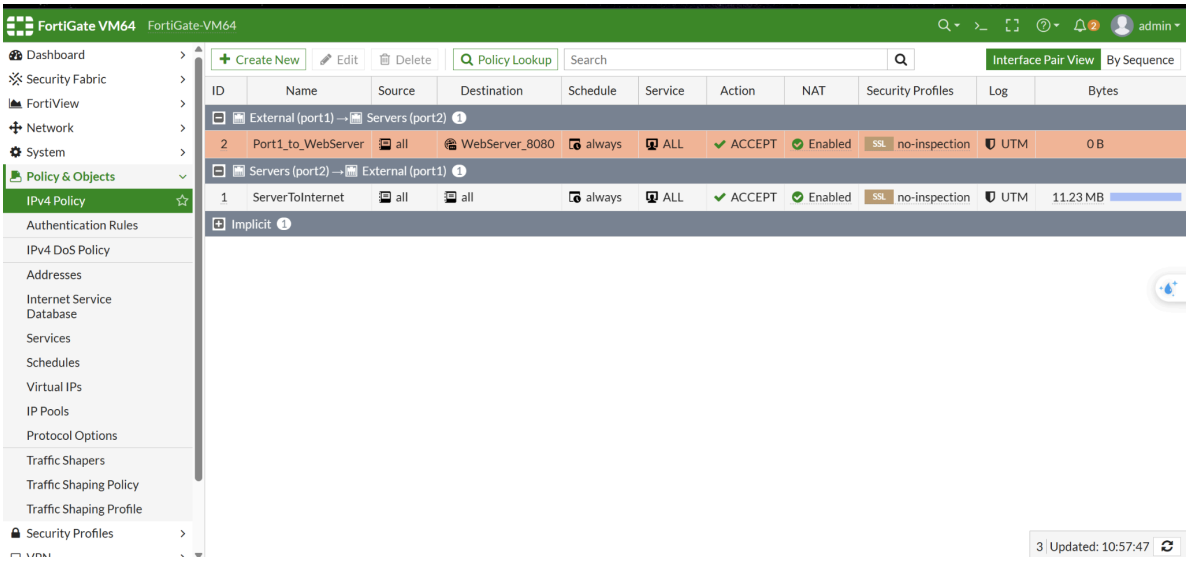
- Name: WebServer_8080
- Interface: port1
- External IP Address/Range: 192.168.1.100
- Mapped IP Address/Range: 10.0.0.3
- Port Forwarding: Enable
- External Service Port: 8080
- Map to Port: 80
- Click OK



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





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