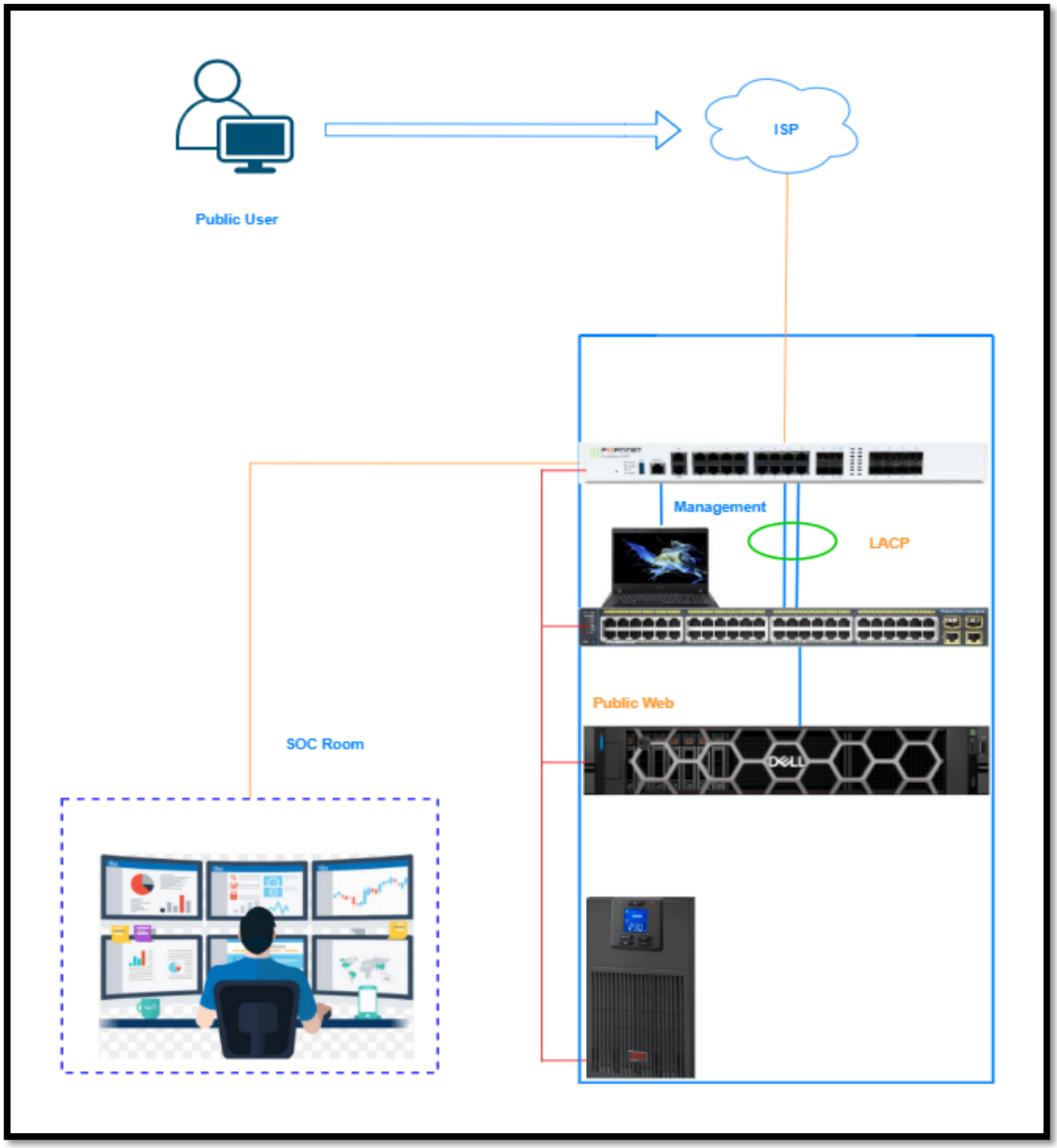
FortiGate Configuration

(Mini DC Project)



Job Requirements

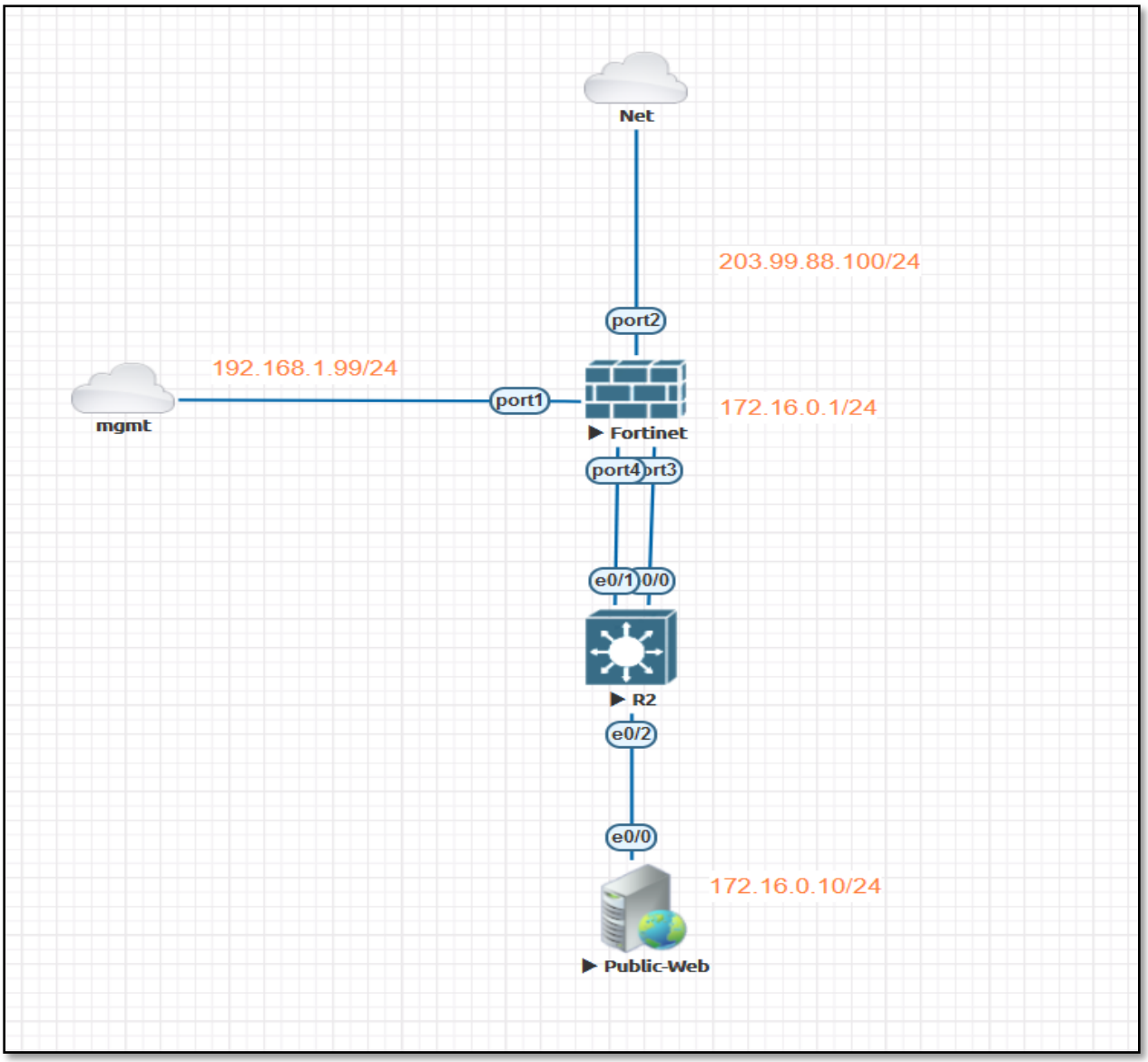
Customer have 1 Dell server, 1 Cisco Catalyst Switch, 1 FortiGate 200F Firewall. Customer want to use Secure LAN network for Internet Access and also want to public their private web-Server.

Service Component

1. Management Configuration
2. Interface & Basic Configuration
3. LACP
4. NAT Policy
5. Port Forwarding
6. Logging
7. Service Testing

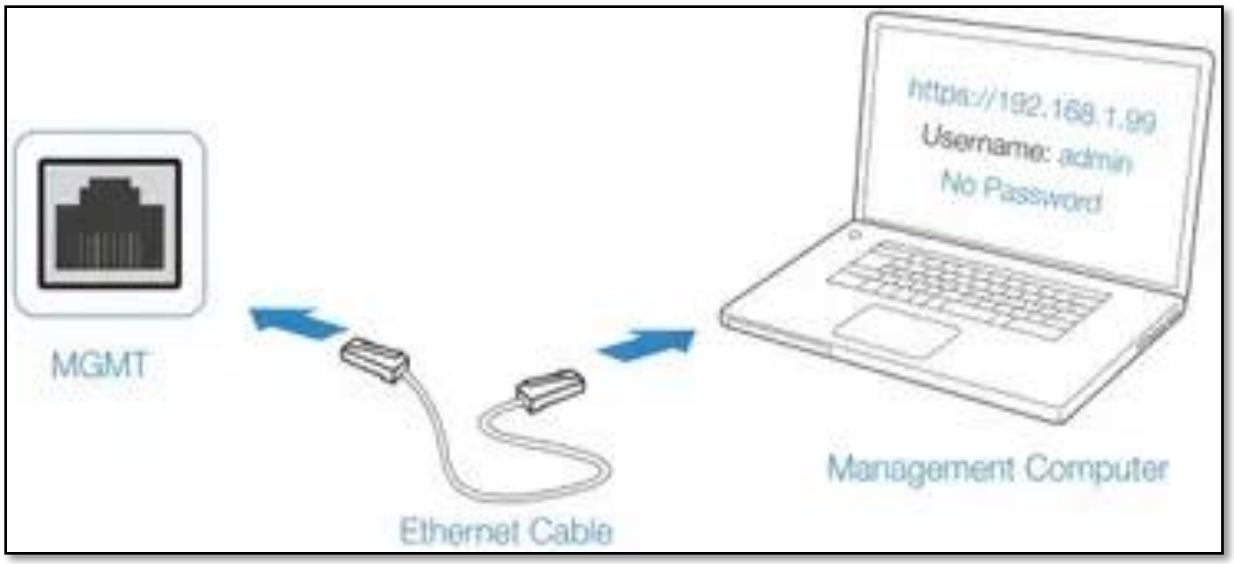
IP Address List

No	Zone Name	IP Address	Gateway	Remark
1	WAN	203.99.88.100/24	203.99.88.2	
2	Mgmt	192.168.1.99/24		
3	LACP			Port 3-4
4	Service	172.16.0.1/24	172.16.0.1	VLAN
5	Web-Server	172.16.0.10/24	172.16.0.1	



1. Initial Configuration

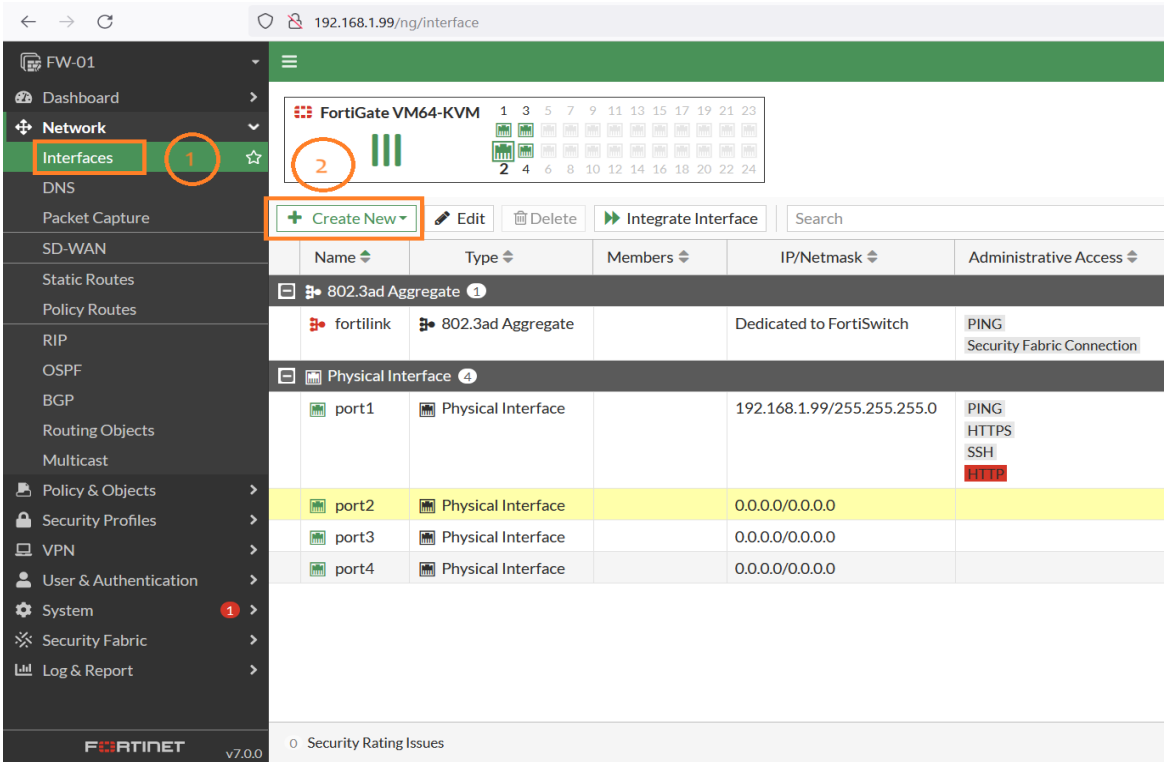
- Connect to “MGMT” interface
- Set IP Address “ 192.168.1.100/24 ” on management PC



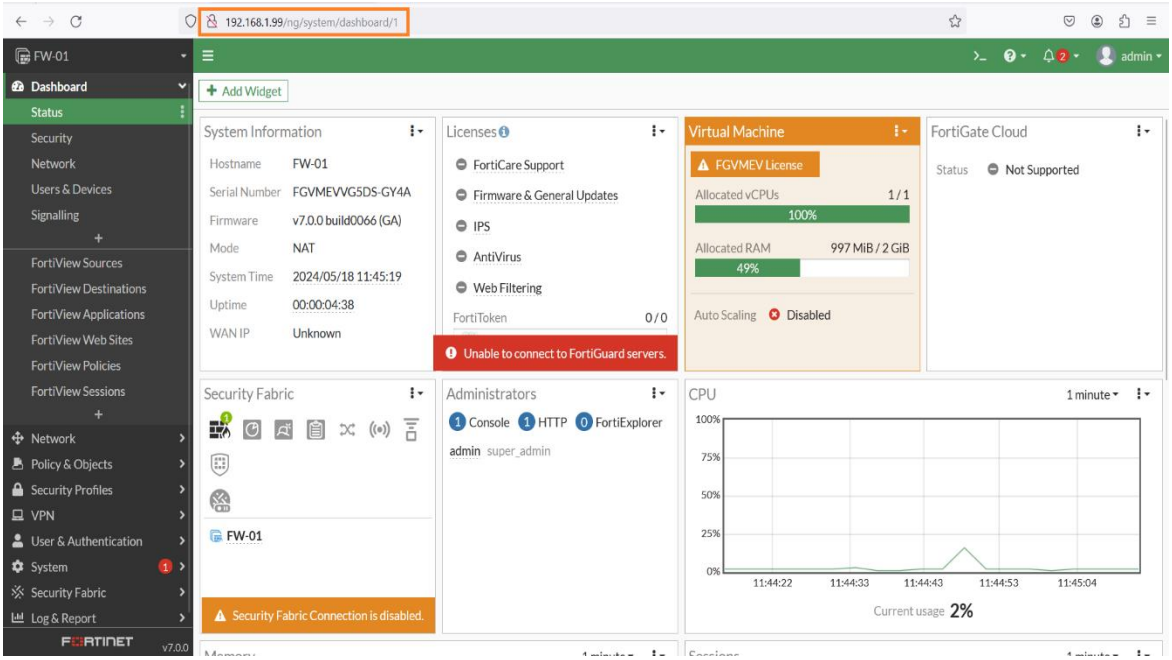
Manual Configuration [via Console]

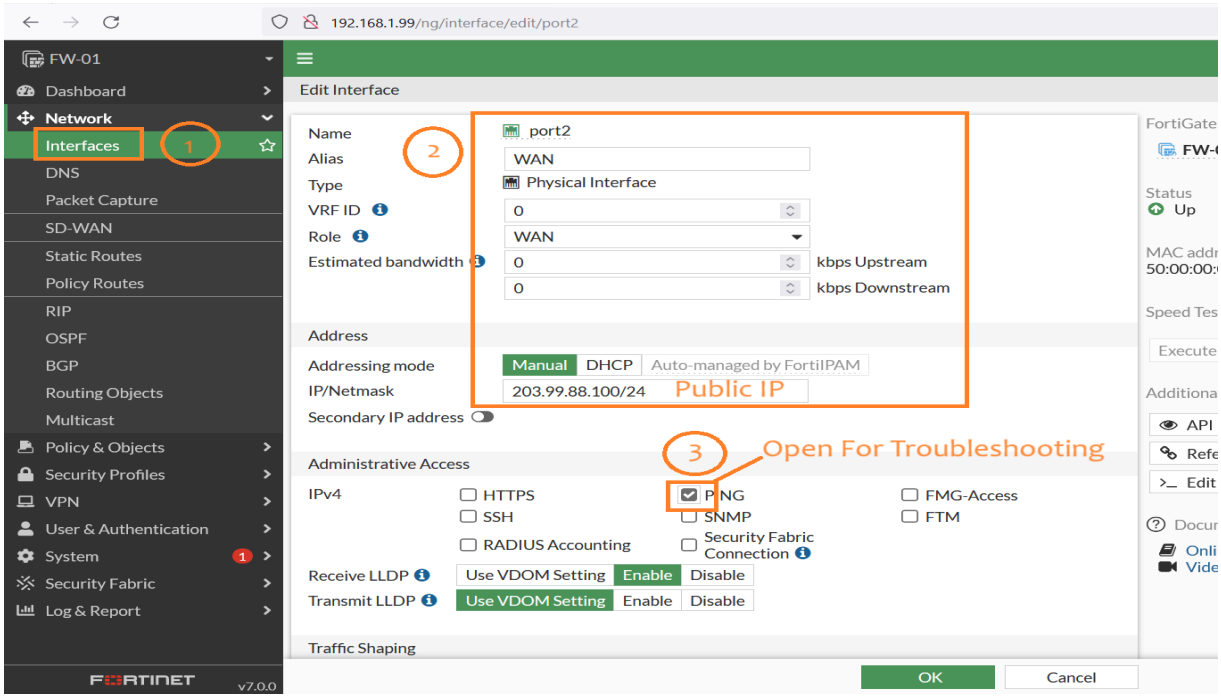
```
FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port1

FortiGate-VM64-KVM (port1) # set mode static

FortiGate-VM64-KVM (port1) # set ip 192.168.1.99/24

FortiGate-VM64-KVM (port1) # set allowaccess https http ping ssh

FortiGate-VM64-KVM (port1) # end

FortiGate-VM64-KVM #
```

2. Login to “FortiGate “
   - browse https://192.168.1.99
   - Username “ admin” Password “no password”

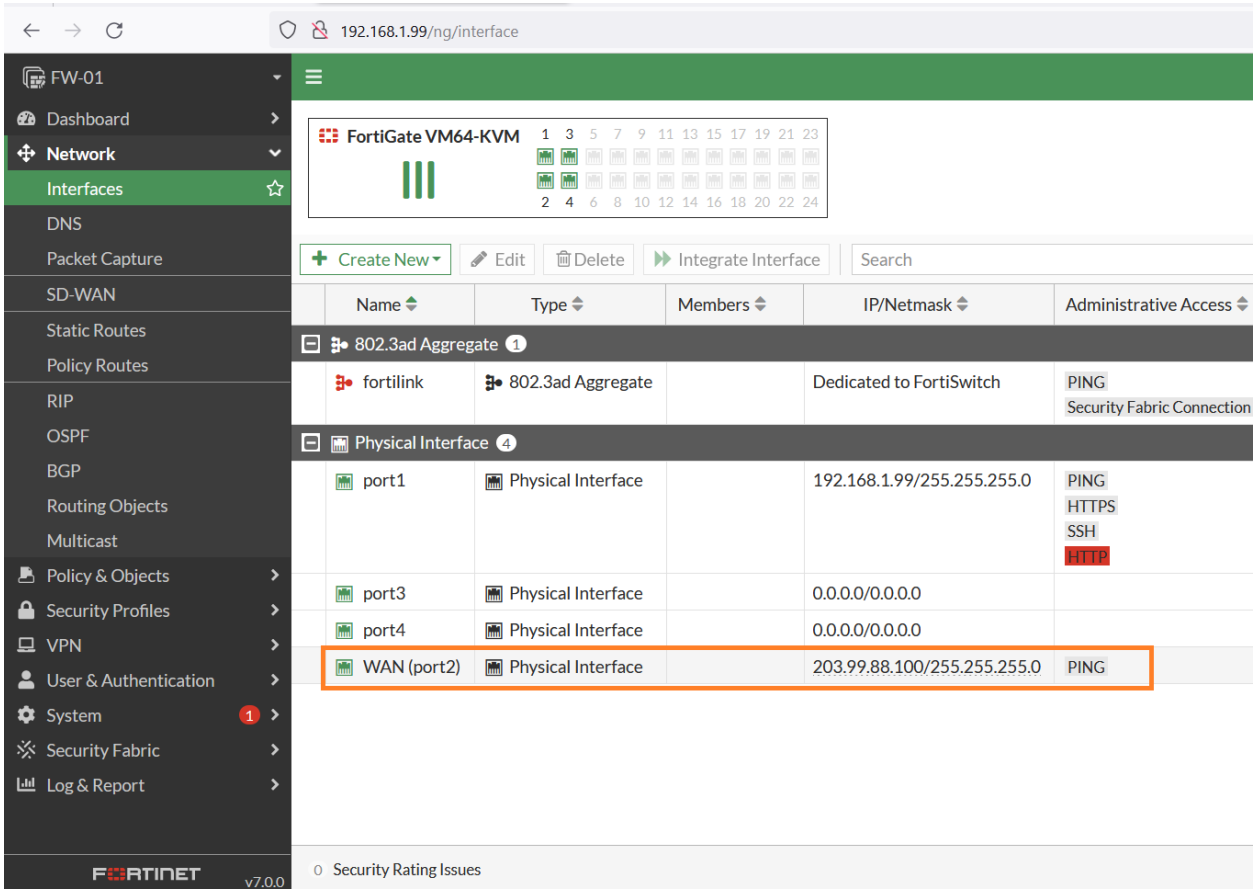


3. Configure Interface

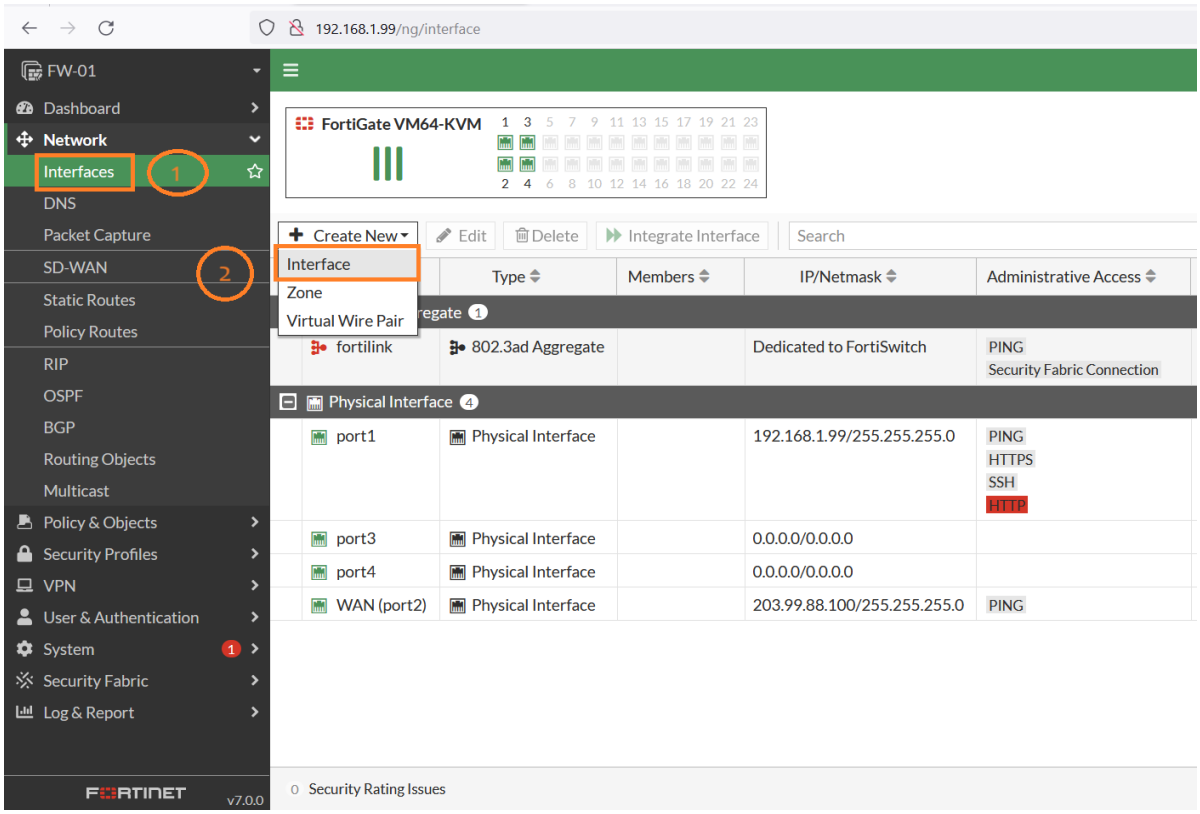




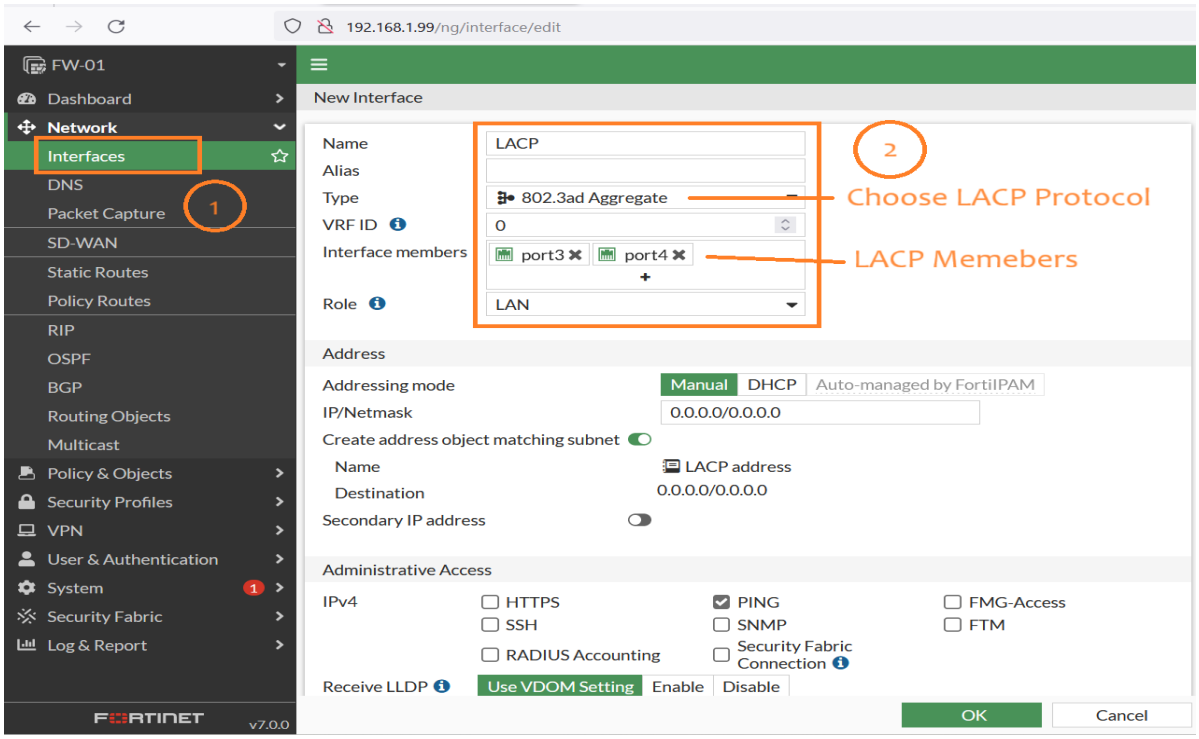
Interface Ready For " WAN"



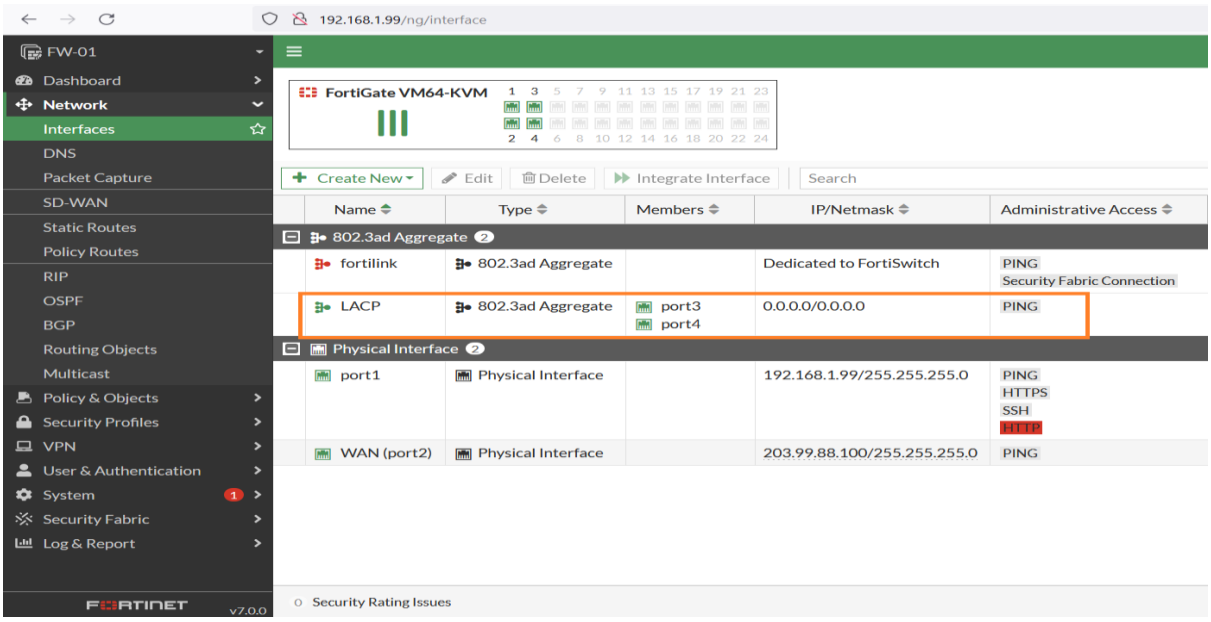
4. Configure LAN interface



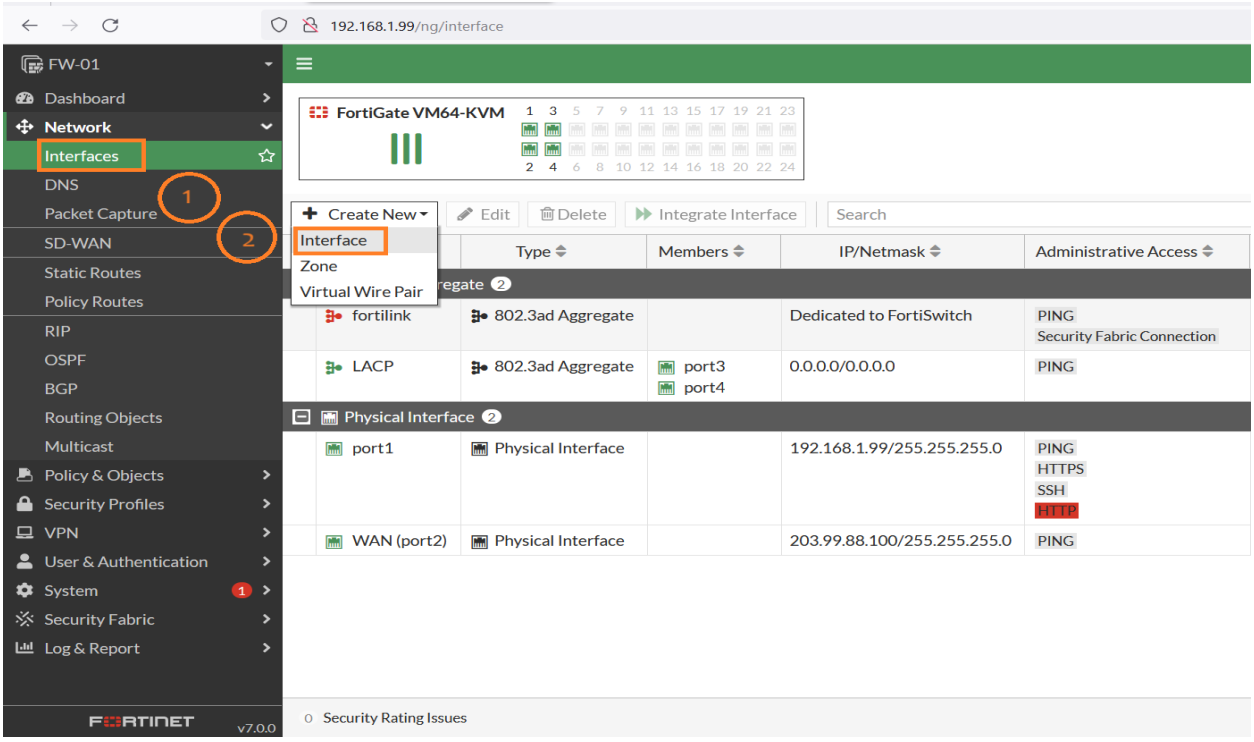
Configure "Aggregate Interface"

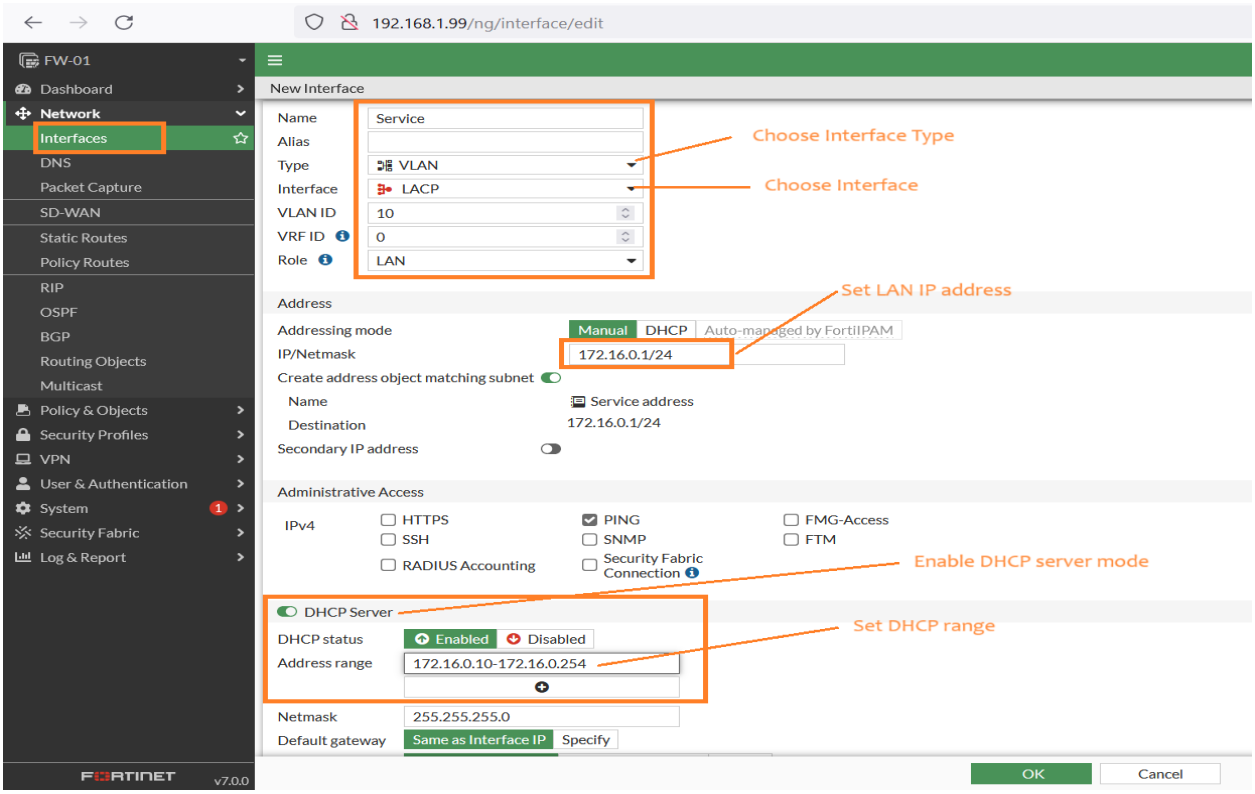


"Aggreate" interface ready

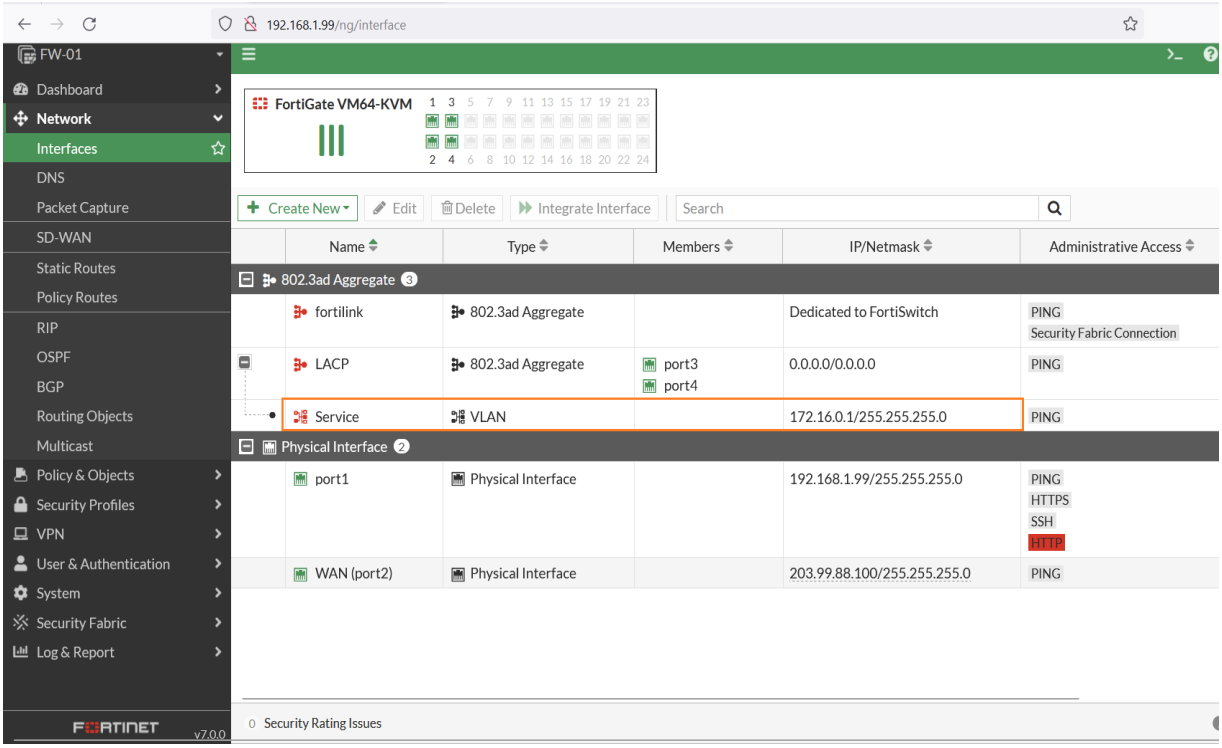


5. Create VLAN for Service Network

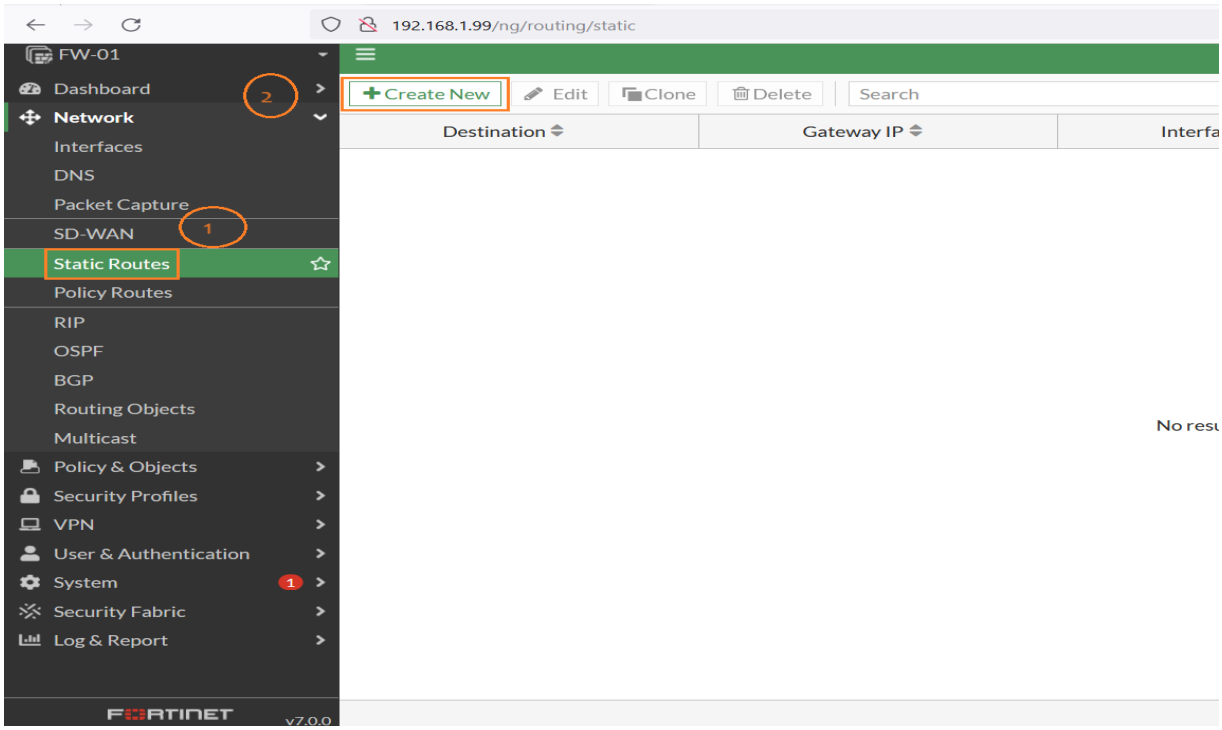


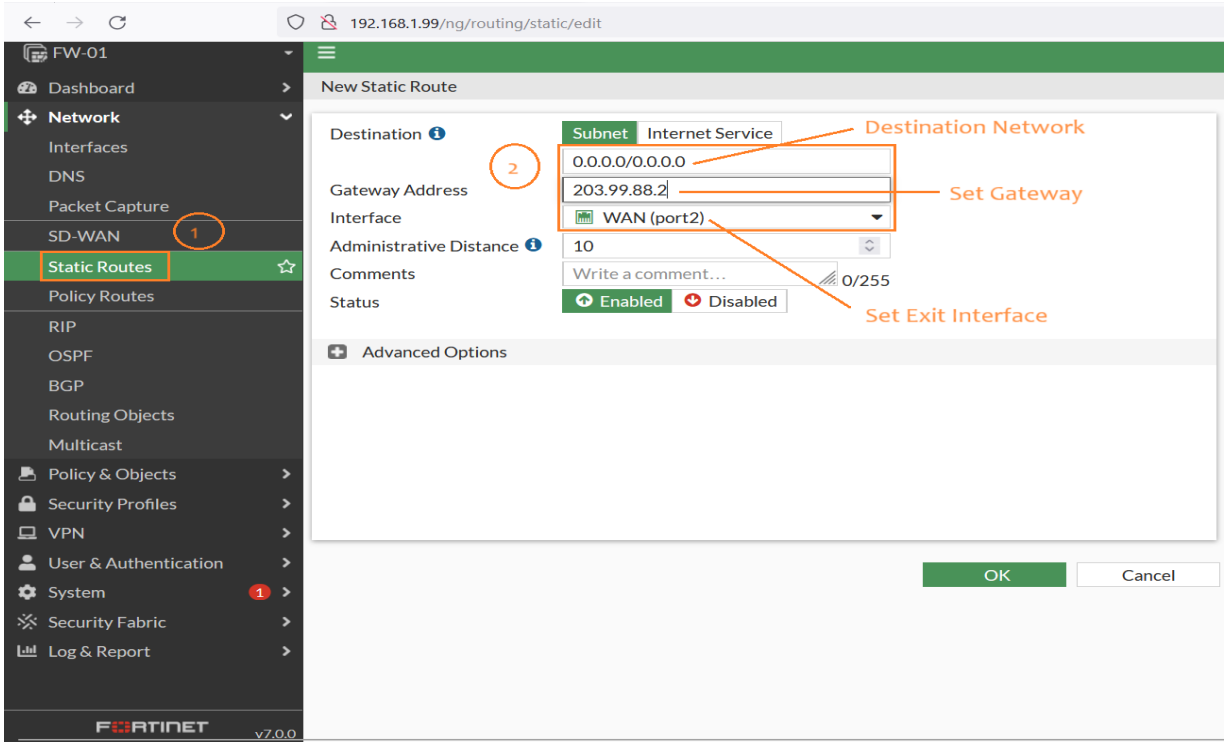


Service VLAN Ready

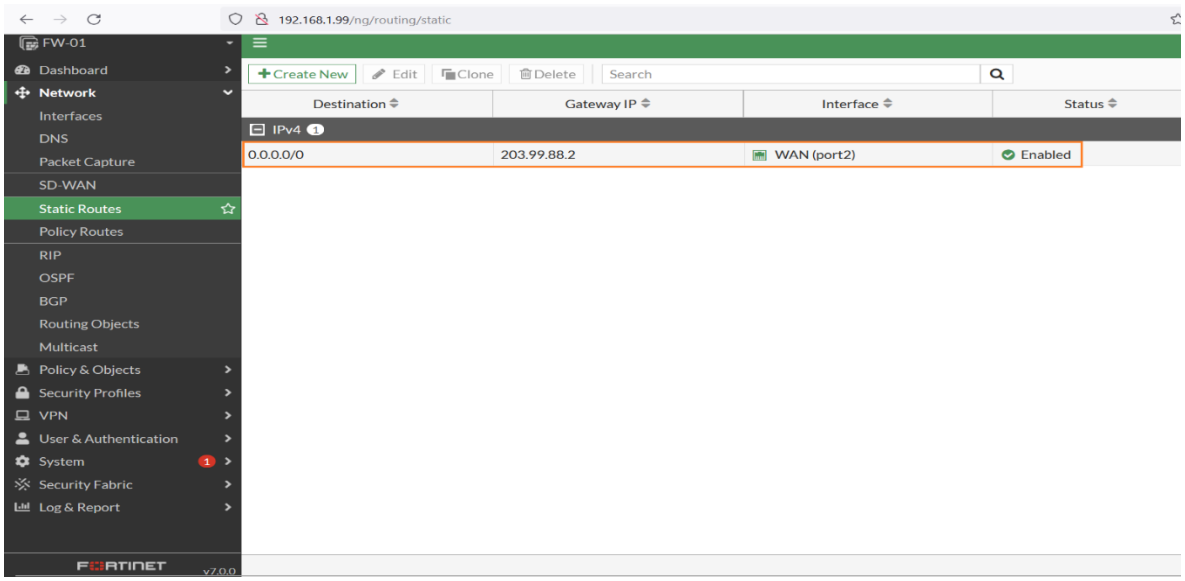


6. Configure Static Route
   Go to Network>Static Routes>Create

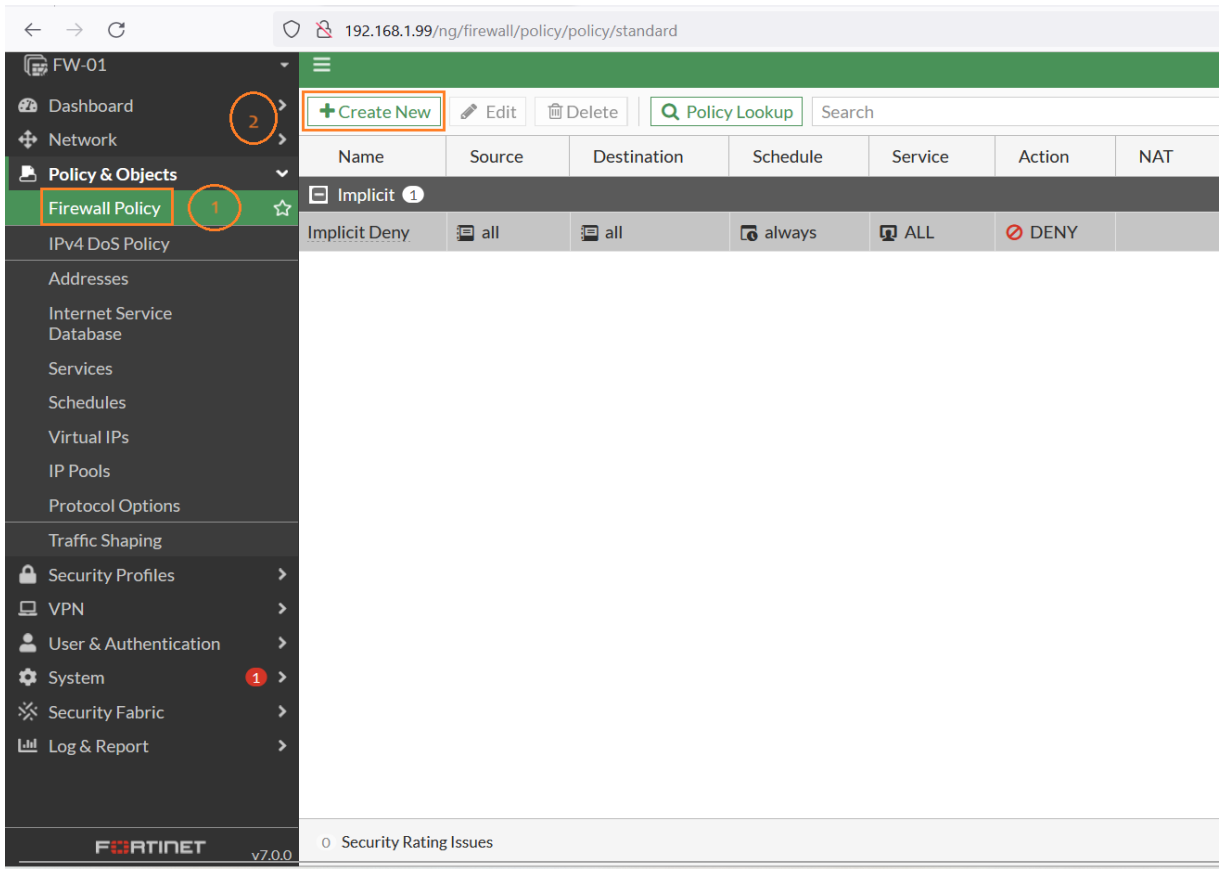


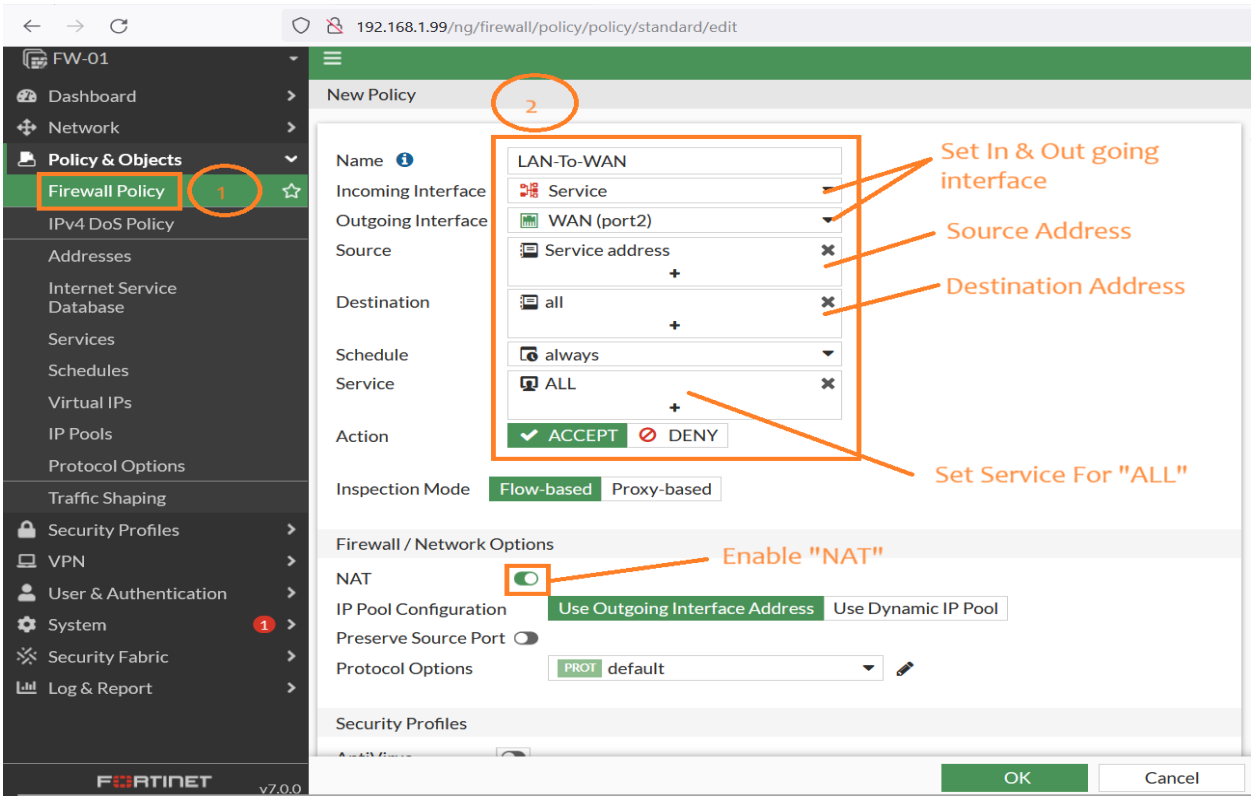


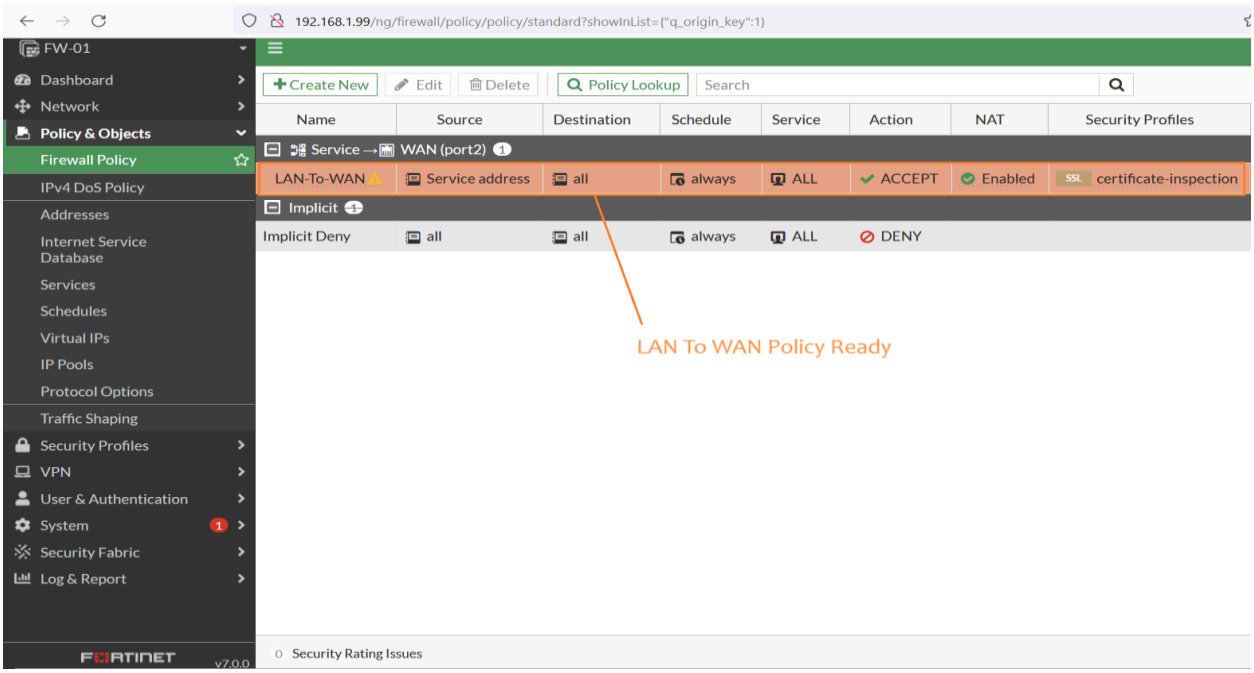
Static Route Ready



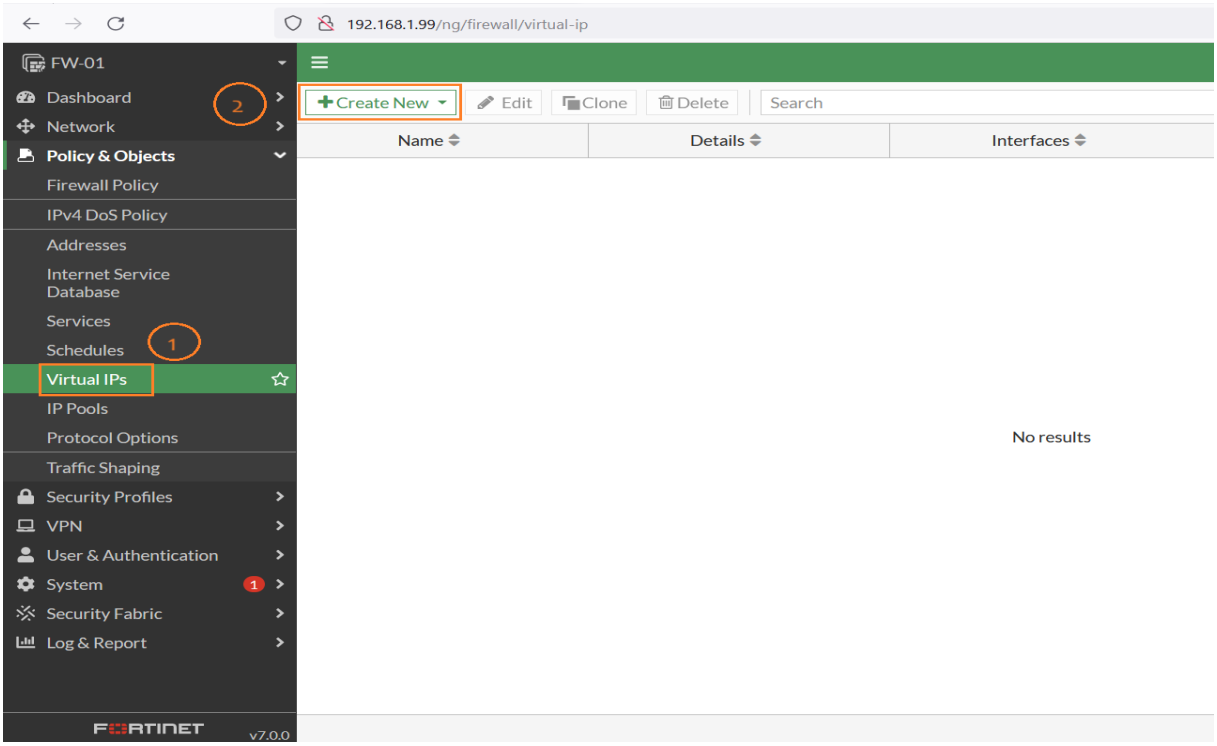
Firewall Policy For "LAN-To-WAN"



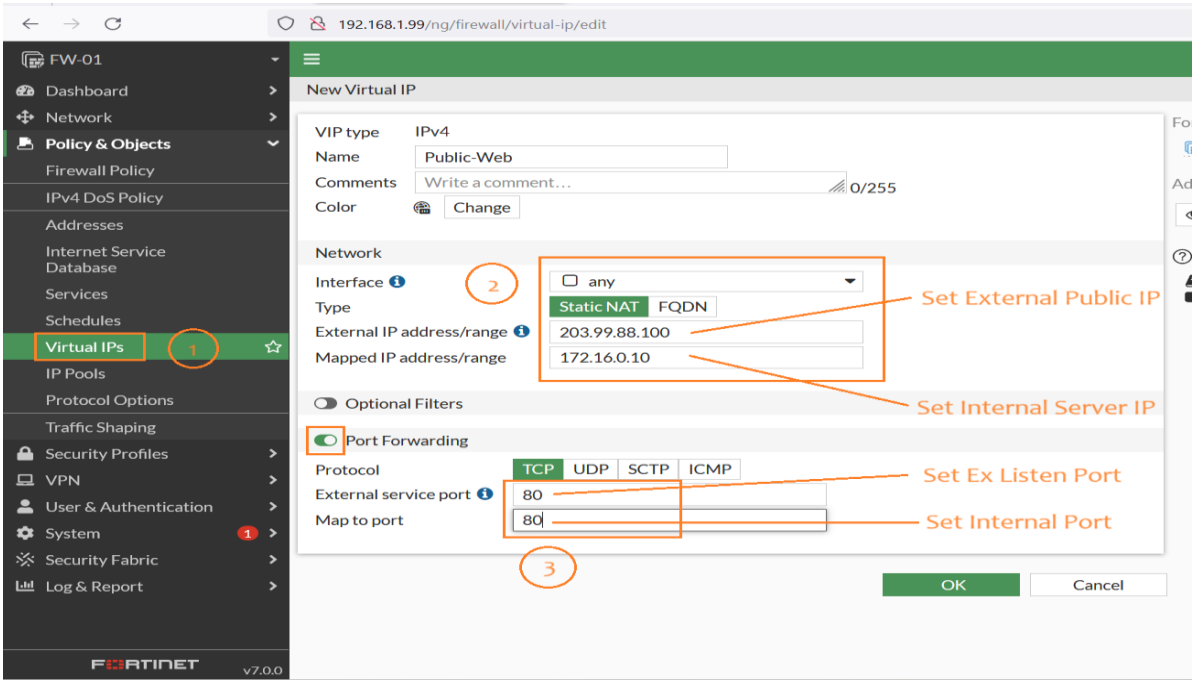

192.168.1.99/ng/firewall/policy/policy/standard/edit
FW-01
Dashboard
Network
Policy & Objects
Firewall Policy
1
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
New Policy
2
Name
LAN-To-WAN
Incoming Interface
Service
Outgoing Interface
WAN (port2)
Source
Service address
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Set In & Out going interface
Source Address
Destination Address
Set Service For "ALL"
Firewall / Network Options
NAT
Enable "NAT"
IP Pool Configuration
Use Outgoing Interface Address
Use Dynamic IP Pool
Preserve Source Port
Protocol Options
PROT
default
Security Profiles
OK
Cancel
FORTINET
v7.0.0


192.168.1.99/ng/firewall/policy/policy/standard?showInList={"q_origin_key":1}
FW-01
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
Create New
Edit
Delete
Policy Lookup
Search
Name
Source
Destination
Schedule
Service
Action
NAT
Security Profiles
Service → WAN (port2) 1
LAN-To-WAN
Service address
all
always
ALL
ACCEPT
Enabled
SSL
certificate-inspection
Implicit 4
Implicit Deny
all
all
always
ALL
DENY
LAN To WAN Policy Ready
0 Security Rating Issues
FORTINET
v7.0.0

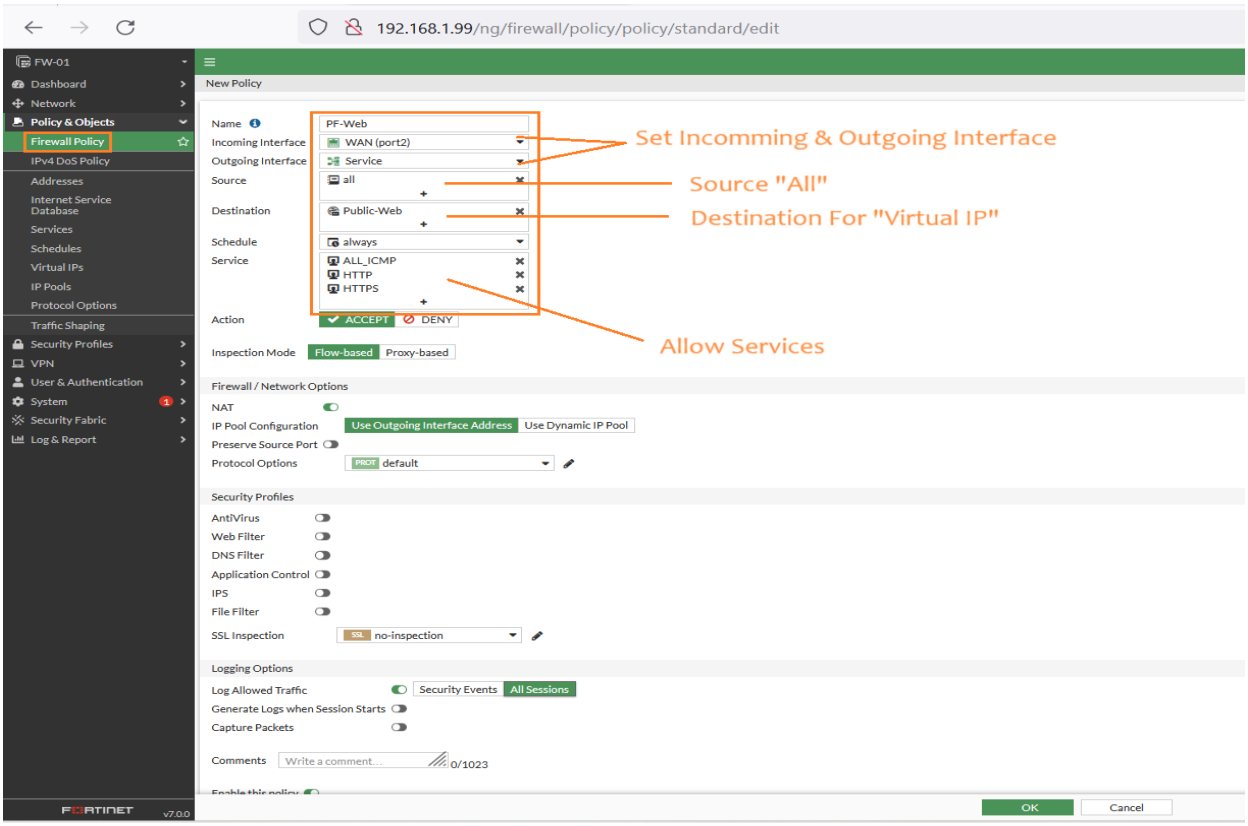
7. Create “Virtual IP”



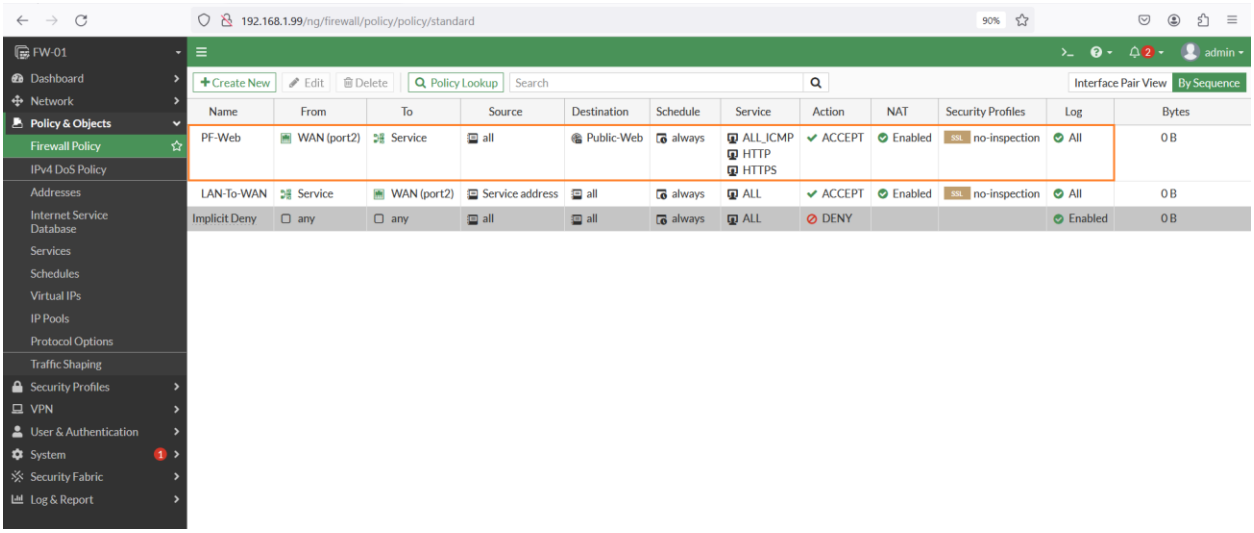
Binding with [external public ip and port] to [internal private ip and port]



Create Port Forwarding Firewall Policy For “Public



Policy Ready For “WAN-To-LAN” DNAT



8. LACP configuration on cisco switch

Port-Channel Configuration

```
Switch(config)#hostname CS
CS(config)#int range eth 0/0-1
CS(config-if-range)#desc /// AGG-TO-FGT ///
CS(config-if-range)#channel-group 10 mode active
exit
```

Trunk Configuration on "Agg Interface"

```
CS(config)#int port-channel 10
CS(config-if)#description /// AGG-TO-FGT ///
CS(config-if)#switchport trunk encapsulation dot1q
CS(config-if)#switchport mode trunk
CS(config-if)#exit
```

Create Vlan [Service vlan 10]

```
CS(config)#vlan 10
CS(config-vlan)#name SERVICE
CS(config-vlan)#exit
CS(config)#
```

Create Access Vlan 10

```
CS(config)#int eth 0/2
CS(config-if)#no sh
CS(config-if)#desc /// TO WEB-SERVER ///
CS(config-if)#switchport mode access
CS(config-if)#switchport access vlan 10
CS(config-if)#switchport nonegotiate
CS(config-if)#exit
CS(config)#
```

Check Etherchannel Status

```
CS#sh etherchannel summary
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
```

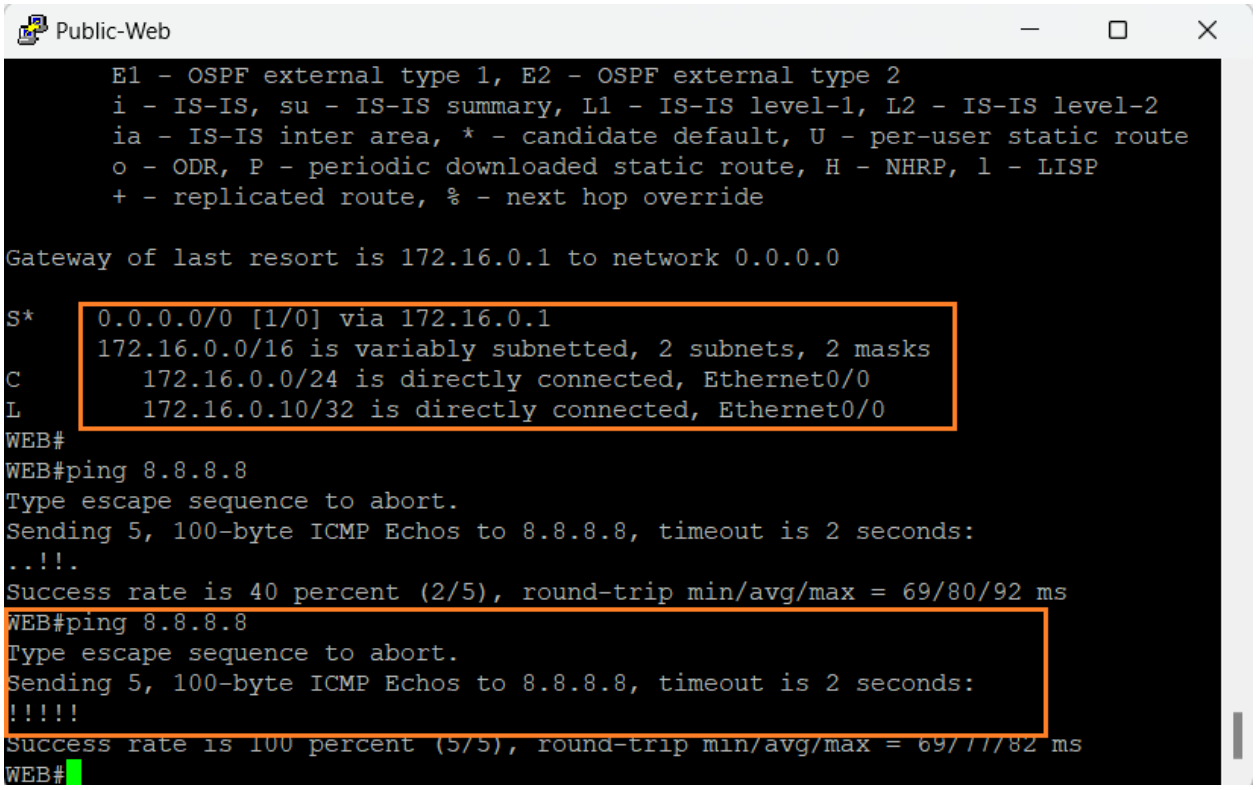
```
10    Po10(SU)       LACP      Et0/0(P)    Et0/1(P)
```

Check Trunk Status

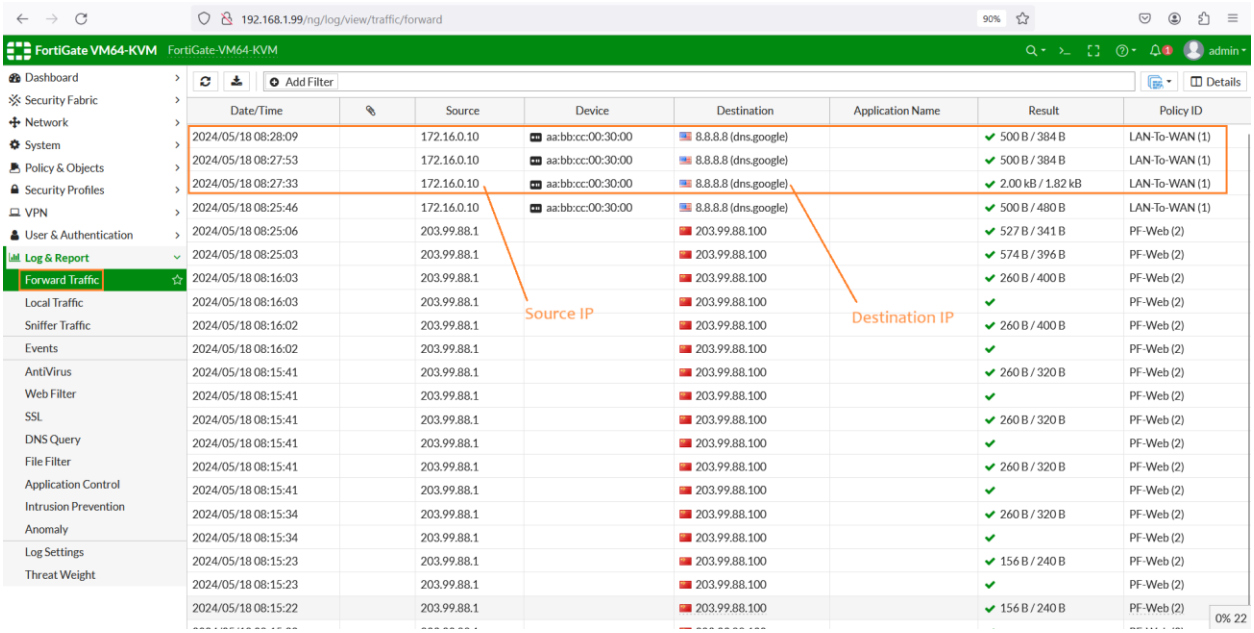
```
CS#show int trunk

Port        Mode             Encapsulation  Status        Native vlan
Po10        on               802.1q         trunking      1

Port        Vlans allowed on trunk
Po10        10

Port        Vlans allowed and active in management domain
Po10        10

Port        Vlans in spanning tree forwarding state and not pruned
Po10        10
```

Service Testing

Ping Test From "LAN" to "8.8.8.8"

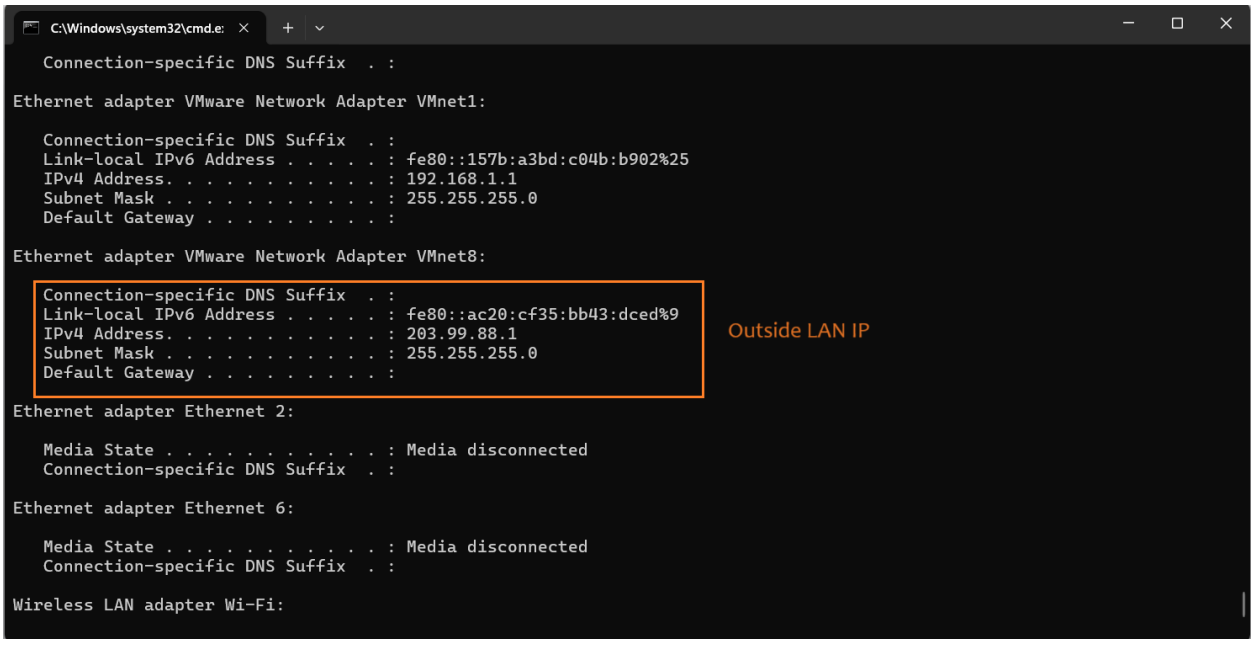


Check Logging From " LAN-172.16.0.10" To "8.8.8.8"

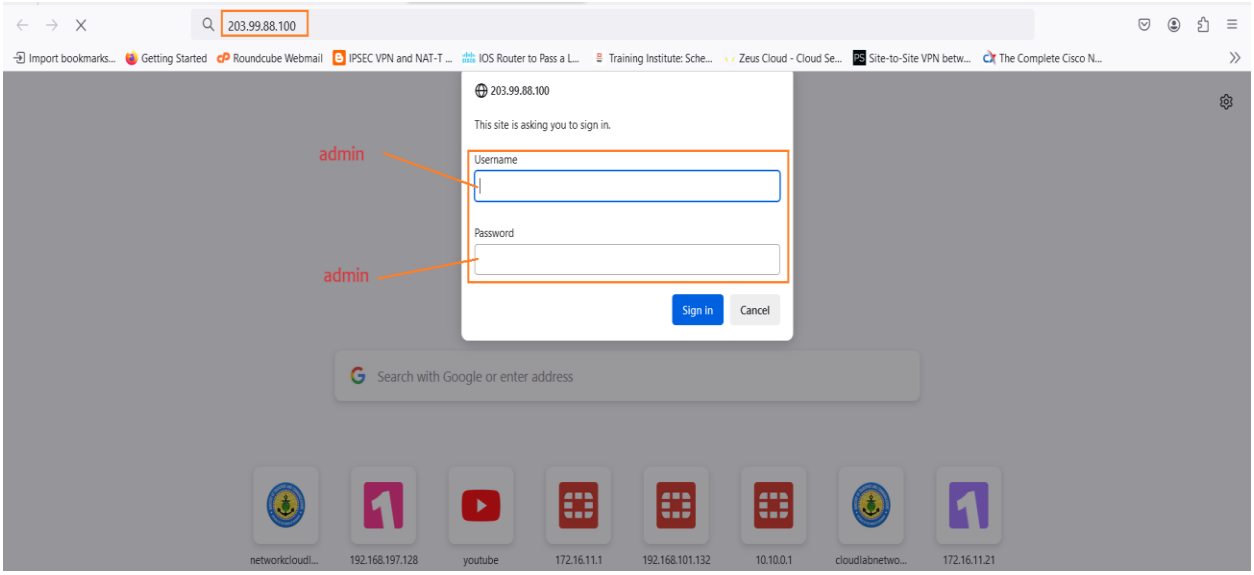


Check Public Web Server Access From "Public"

Check Lan IP



Browse to Public IP (WAN IP)



Successfully Access to [Private Web-Server] From [Public]