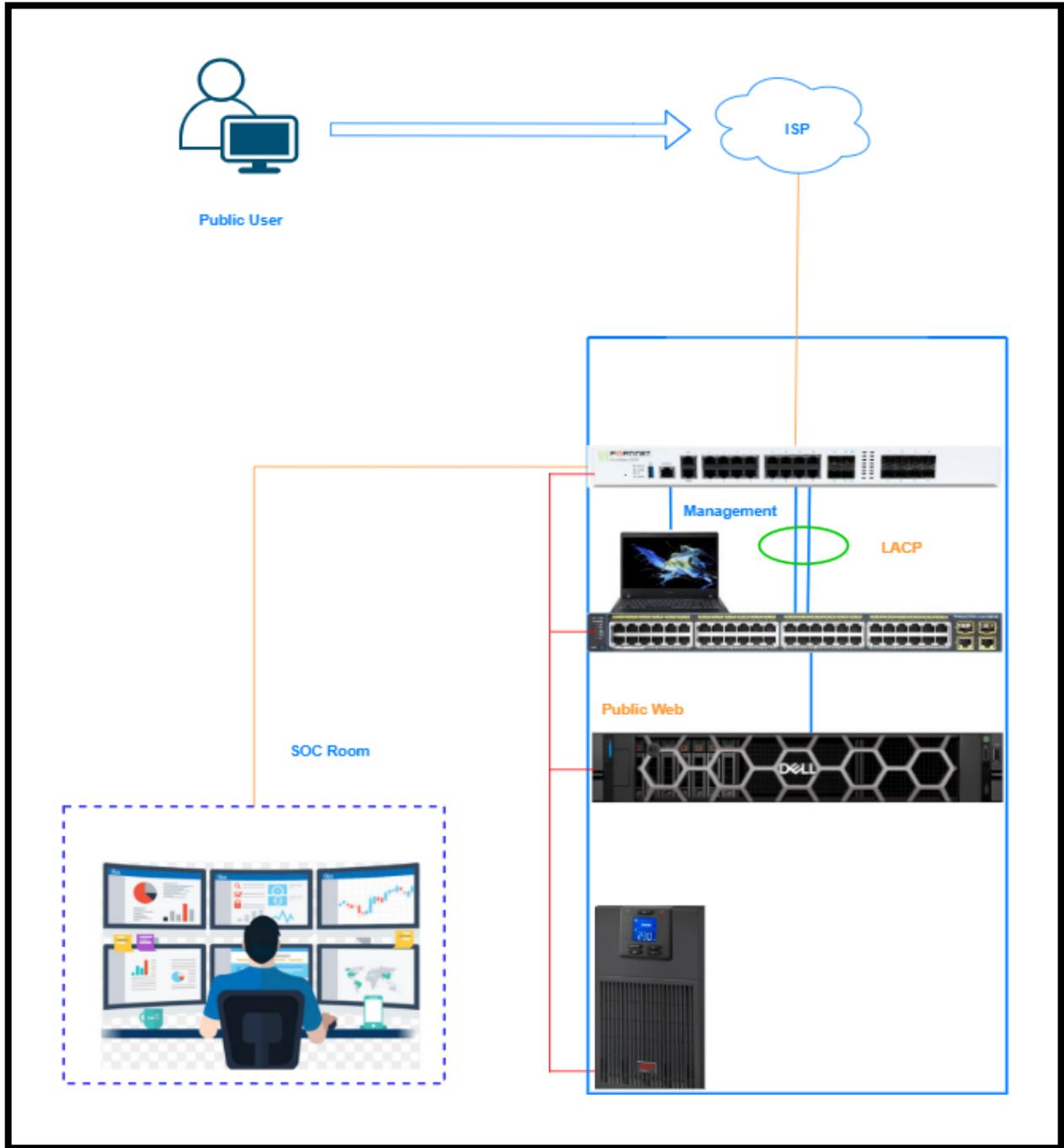


# FortiGate Configuration (Mini DC Project)



## Job Requirements

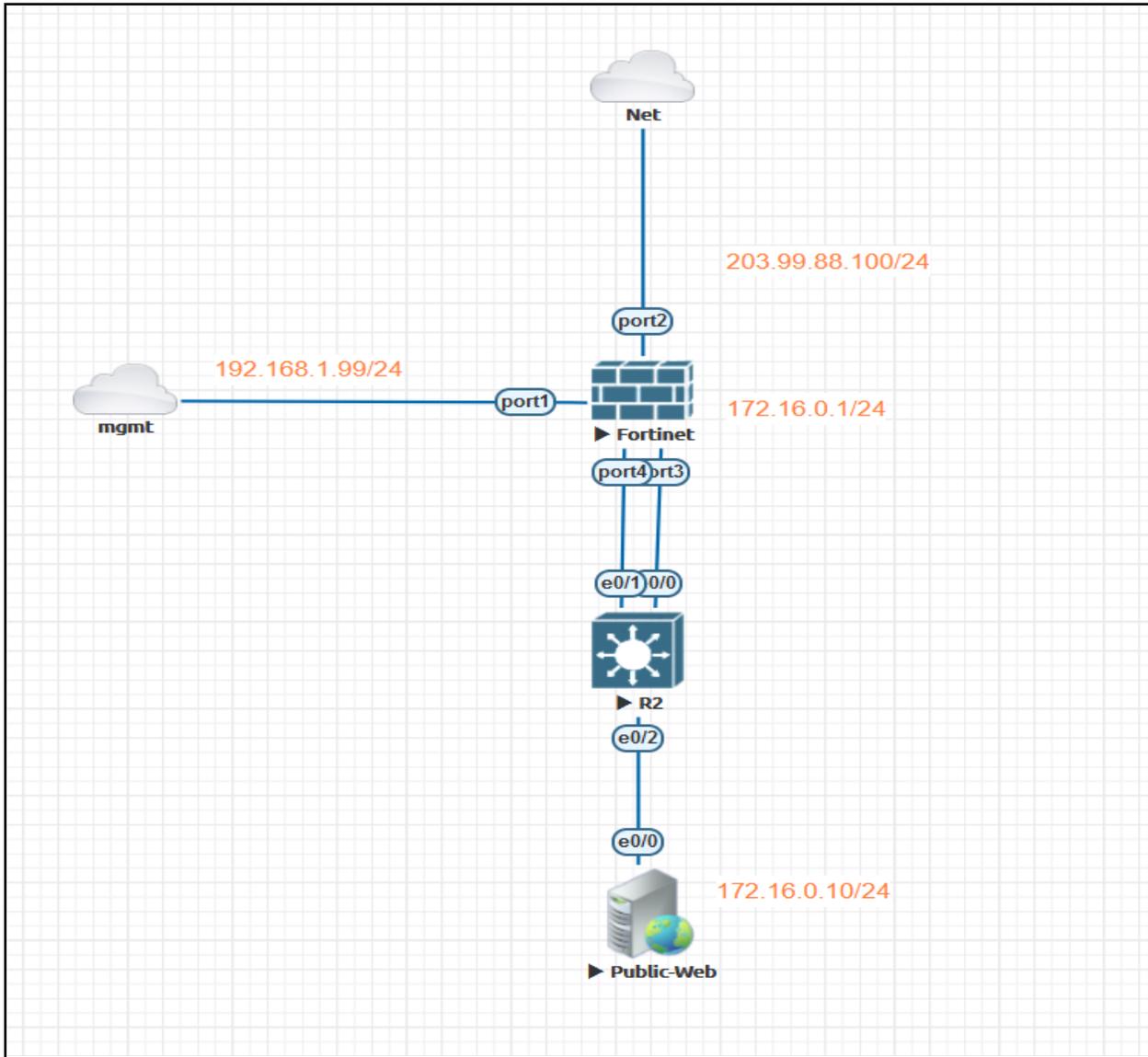
Customer have 1 Dell server, 1 Cisco Catalyst Switch, 1 FortiGate 200F Firewall.  
Customer want to use Secure LAN network for Internet Access and also want to public their private web-Server.

## 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

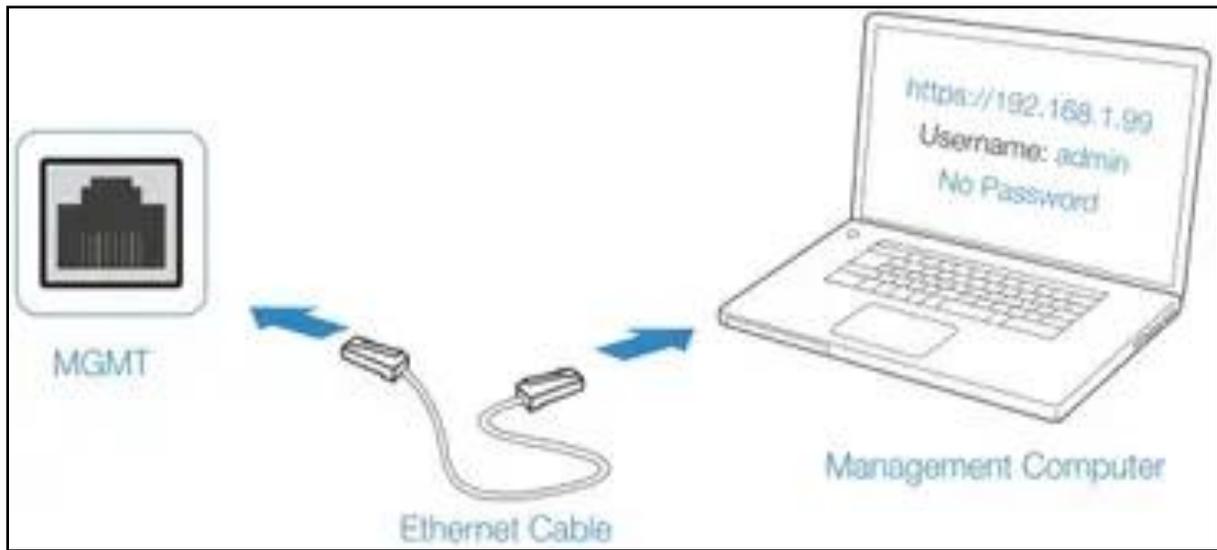
No	Zone Name	IP Address	Gateway	Remark
1	WAN	203.99.88.100/24	203.99.88.2	
2	Mgmt	192.168.1.99/24		
3	LACP			Port 3-4
4	Service	172.16.0.1/24	172.16.0.1	VLAN
5	Web-Server	172.16.0.10/24	172.16.0.1	



## 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”

Name	Type	Members	IP/Netmask	Administrative Access
<b>802.3ad Aggregate</b> 1				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
<b>Physical Interface</b> 4				
port1	Physical Interface		192.168.1.99/255.255.255.0	PING HTTPS SSH HTTP
port2	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	

## 3. Configure Interface

System Information

- Hostname: FW-01
- Serial Number: FGMEVVG5DS-GY4A
- Firmware: v7.0.0 build0066 (GA)
- Mode: NAT
- System Time: 2024/05/18 11:45:19
- Uptime: 00:00:04:38
- WAN IP: Unknown

Licenses

- FortiCare Support
- Firmware & General Updates
- IPS
- AntiVirus
- Web Filtering
- FortiToken: 0/0

Virtual Machine

- FGVMEV License
- Allocated vCPUs: 1/1 (100%)
- Allocated RAM: 997 MiB / 2 GiB (49%)
- Auto Scaling: Disabled

FortiGate Cloud

- Status: Not Supported

Administrators

- Console: 1
- HTTP: 1
- FortiExplorer: 0
- admin: super\_admin

CPU Usage (1 minute)

- Current usage: 2%

192.168.1.99/ng/interface/edit/port2

**Edit Interface**

Name: **port2** (2)

Alias: WAN

Type: Physical Interface

VRF ID: 0

Role: WAN

Estimated bandwidth: 0 kbps Upstream, 0 kbps Downstream

Addressing mode: **Manual** | DHCP | Auto-managed by FortiIPAM

IP/Netmask: 203.99.88.100/24 **Public IP**

Administrative Access:

- IPv4:  HTTPS,  SSH,  **PING** (3) *Open For Troubleshooting*,  SNMP,  FMG-Access,  FTM
- Receive LLDP: Use VDOM Setting | **Enable** | Disable
- Transmit LLDP: Use VDOM Setting | **Enable** | Disable

OK Cancel

## Interface Ready For “WAN”

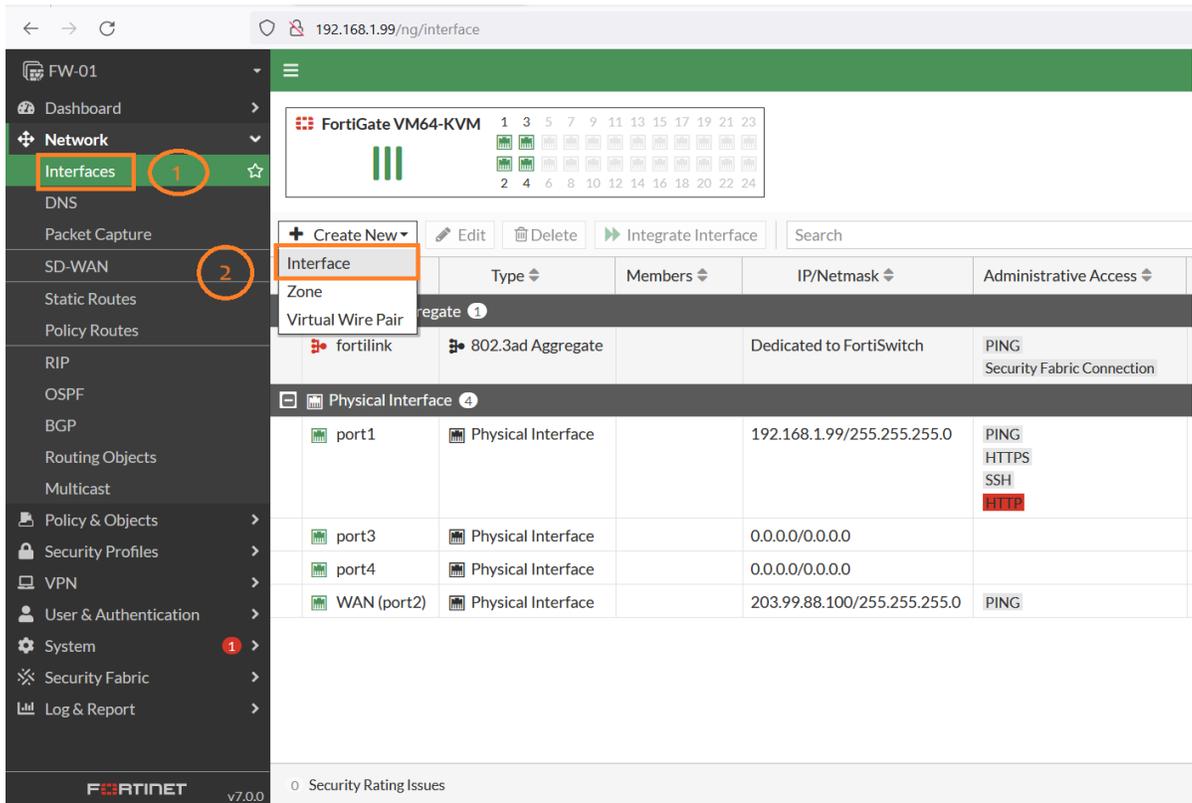
192.168.1.99/ng/interface

FortiGate VM64-KVM

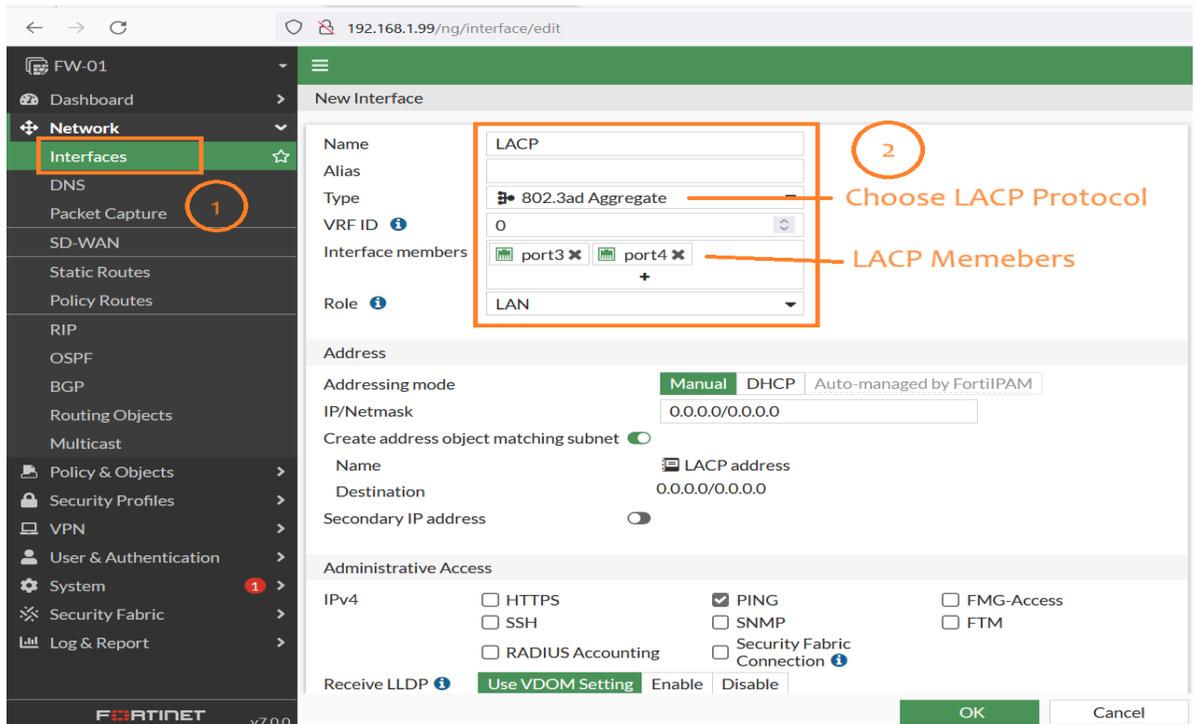
Name	Type	Members	IP/Netmask	Administrative Access
<b>802.3ad Aggregate</b> 1				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
<b>Physical Interface</b> 4				
port1	Physical Interface		192.168.1.99/255.255.255.0	PING HTTPS SSH <b>HTTP</b>
port3	Physical Interface		0.0.0.0/0.0.0.0	
port4	Physical Interface		0.0.0.0/0.0.0.0	
<b>WAN (port2)</b>	<b>Physical Interface</b>		<b>203.99.88.100/255.255.255.0</b>	<b>PING</b>

0 Security Rating Issues

#### 4. Configure LAN interface



#### Configure "Aggregate Interface"



## “Aggregate” interface ready

The screenshot shows the FortiGate GUI for FW-01, specifically the Interfaces page. The left sidebar contains a navigation menu with 'Network' and 'Interfaces' highlighted. The main content area displays a table of interfaces. The 'LACP' interface is highlighted with an orange border. Above the table, there is a 'Create New' dropdown menu with 'Interface' selected. The table has columns for Name, Type, Members, IP/Netmask, and Administrative Access.

Name	Type	Members	IP/Netmask	Administrative Access
<b>802.3ad Aggregate</b>				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
LACP	802.3ad Aggregate	port3 port4	0.0.0.0/0.0.0.0	PING
<b>Physical Interface</b>				
port1	Physical Interface		192.168.1.99/255.255.255.0	PING HTTPS SSH HTTP
WAN (port2)	Physical Interface		203.99.88.100/255.255.255.0	PING

## 5. Create VLAN for Service Network

The screenshot shows the FortiGate GUI for FW-01, specifically the Interfaces page. The left sidebar contains a navigation menu with 'Network' and 'Interfaces' highlighted. The main content area displays a table of interfaces. The 'Create New' dropdown menu is open, and 'Interface' is selected. The table has columns for Name, Type, Members, IP/Netmask, and Administrative Access.

Name	Type	Members	IP/Netmask	Administrative Access
<b>802.3ad Aggregate</b>				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
LACP	802.3ad Aggregate	port3 port4	0.0.0.0/0.0.0.0	PING
<b>Physical Interface</b>				
port1	Physical Interface		192.168.1.99/255.255.255.0	PING HTTPS SSH HTTP
WAN (port2)	Physical Interface		203.99.88.100/255.255.255.0	PING

192.168.1.99/ng/interface/edit

New Interface

Name: Service

Alias:

Type: VLAN (Choose Interface Type)

Interface: LACP (Choose Interface)

VLAN ID: 10

VRF ID: 0

Role: LAN

Address

Addressing mode: Manual | DHCP | Auto-managed by FortiPAM

IP/Netmask: 172.16.0.1/24 (Set LAN IP address)

Create address object matching subnet:

Name: Service address

Destination: 172.16.0.1/24

Secondary IP address:

Administrative Access

IPv4:  HTTPS,  SSH,  RADIUS Accounting,  PING,  SNMP,  Security Fabric Connection,  FMG-Access,  FTM

DHCP Server:  (Enable DHCP server mode)

DHCP status: Enabled (Set DHCP range)

Address range: 172.16.0.10-172.16.0.254

Netmask: 255.255.255.0

Default gateway: Same as Interface IP | Specify

OK Cancel

## Service VLAN Ready

192.168.1.99/ng/interface

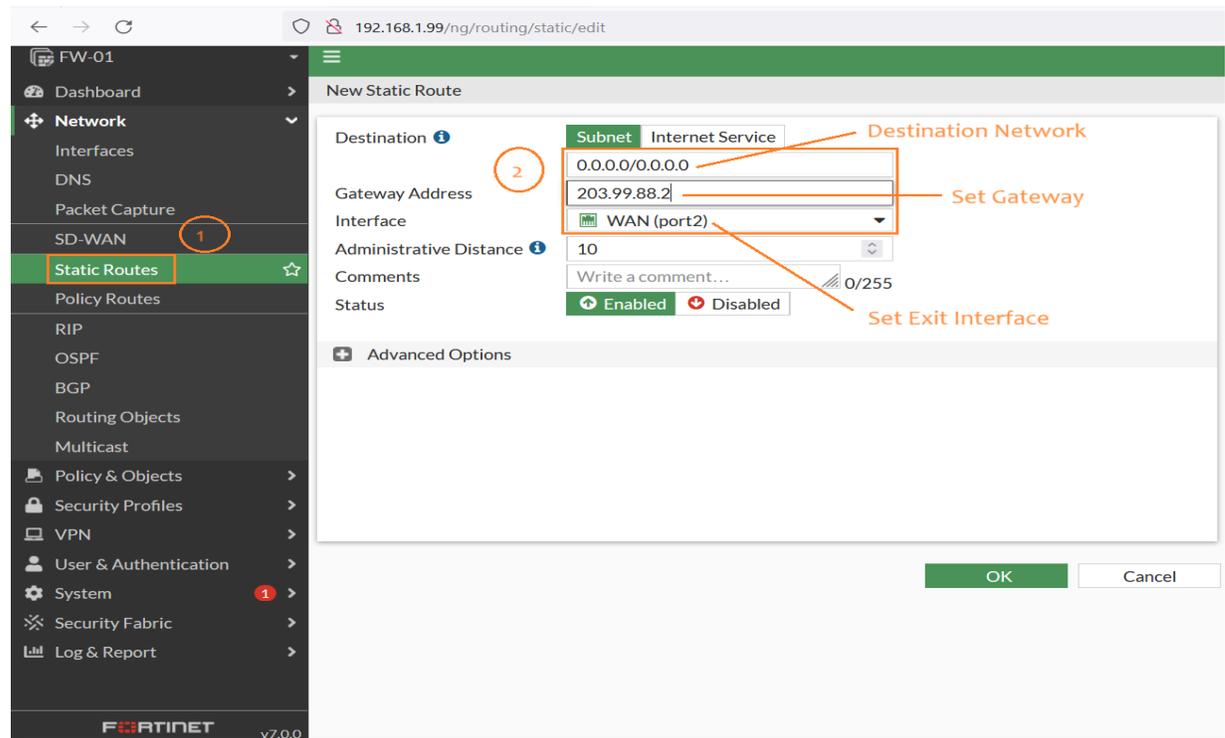
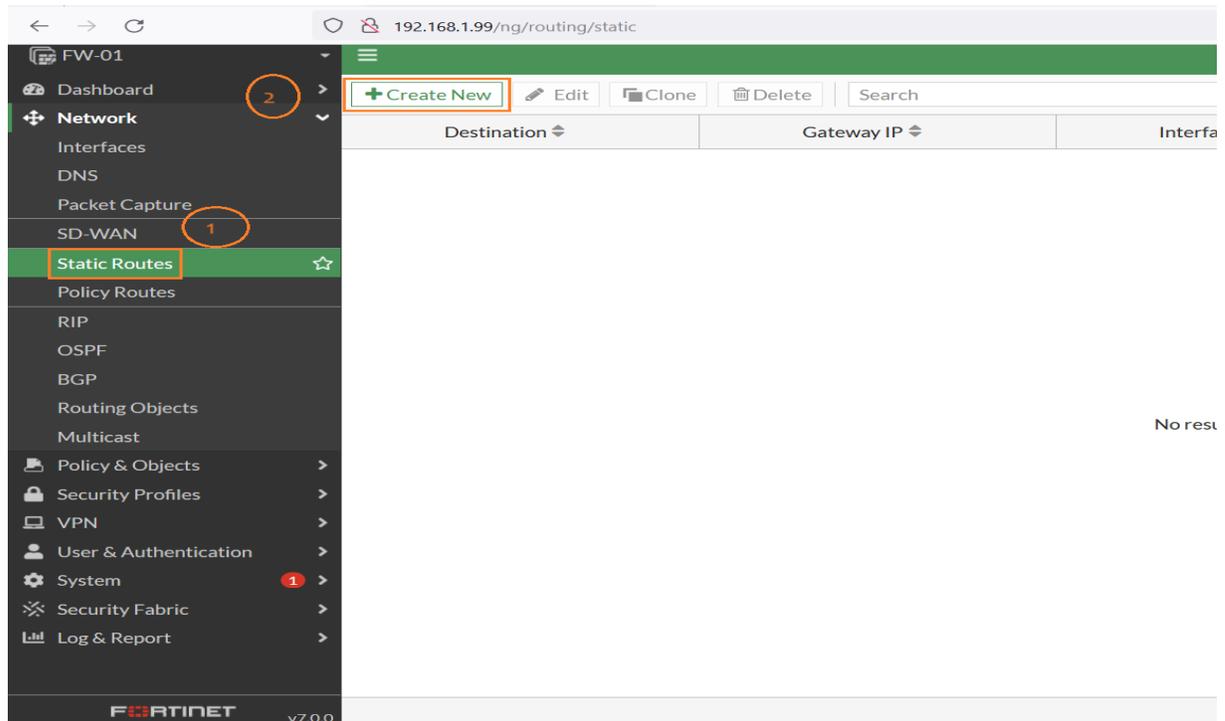
FortiGate VM64-KVM

Name	Type	Members	IP/Netmask	Administrative Access
802.3ad Aggregate	802.3ad Aggregate			
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
LACP	802.3ad Aggregate	port3 port4	0.0.0.0/0.0.0.0	PING
Service	VLAN		172.16.0.1/255.255.255.0	PING
Physical Interface	Physical Interface			
port1	Physical Interface		192.168.1.99/255.255.255.0	PING HTTPS SSH HTTP
WAN (port2)	Physical Interface		203.99.88.100/255.255.255.0	PING

0 Security Rating Issues

## 6. Configure Static Route

Go to **Network>Static Routes>Create**



## Static Route Ready

The screenshot shows the Fortinet web interface for configuring static routes. The left sidebar is expanded to 'Static Routes'. The main content area displays a table with the following data:

Destination	Gateway IP	Interface	Status
0.0.0.0/0	203.99.88.2	WAN (port2)	Enabled

## Firewall Policy For "LAN-To-WAN"

The screenshot shows the Fortinet web interface for configuring a firewall policy. The left sidebar is expanded to 'Policy & Objects', and 'Firewall Policy' is selected. The main content area displays a table with the following data:

Name	Source	Destination	Schedule	Service	Action	NAT
Implicit 1	all	all	always	ALL	DENY	

Annotations in the image include a red circle '1' around 'Firewall Policy' in the sidebar and a red circle '2' around the '+ Create New' button in the top toolbar.

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 (1)
- 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 (checked), DENY

Inspection Mode: Flow-based (selected), Proxy-based

Firewall / Network Options

NAT:  Enable "NAT"

IP Pool Configuration: Use Outgoing Interface Address (selected), Use Dynamic IP Pool

Preserve Source Port:

Protocol Options: PROT default

Security Profiles

OK Cancel

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 (1)
- Security Fabric
- Log & Report

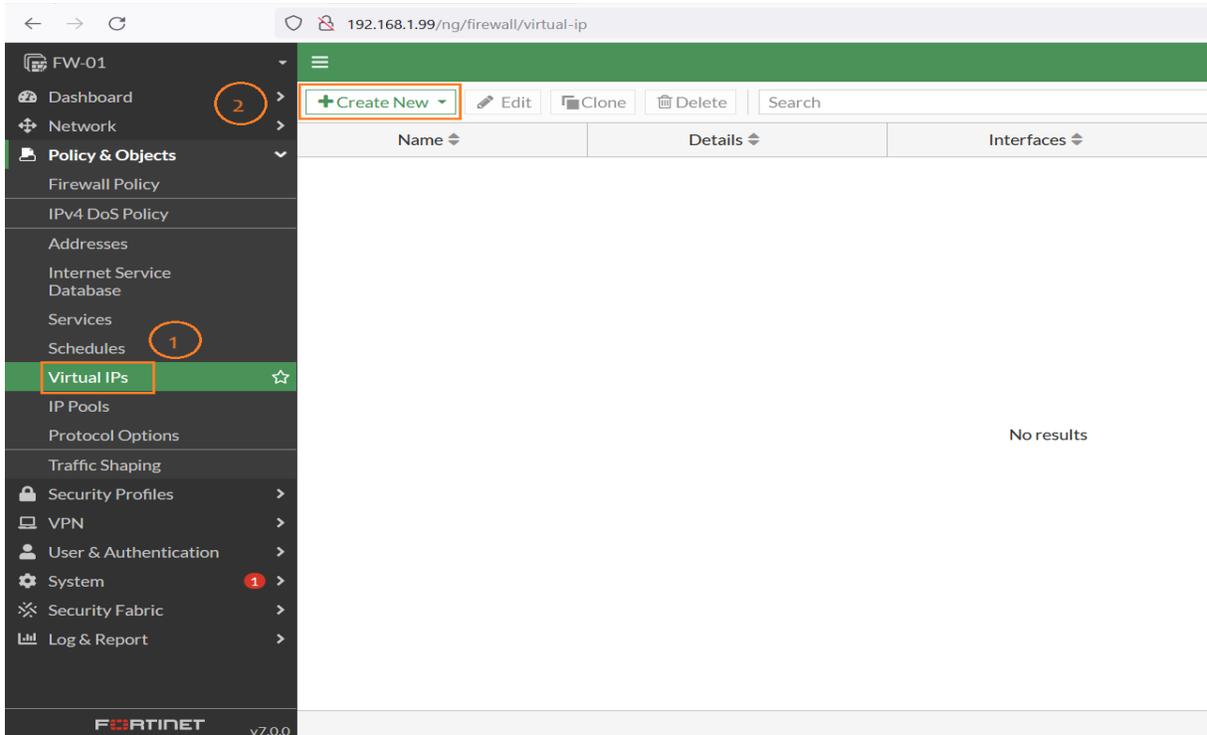
Policy Lookup

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
Service → WAN (port2)							
LAN-To-WAN	Service address	all	always	ALL	ACCEPT	Enabled	SSL certificate-inspection
Implicit Deny	all	all	always	ALL	DENY		

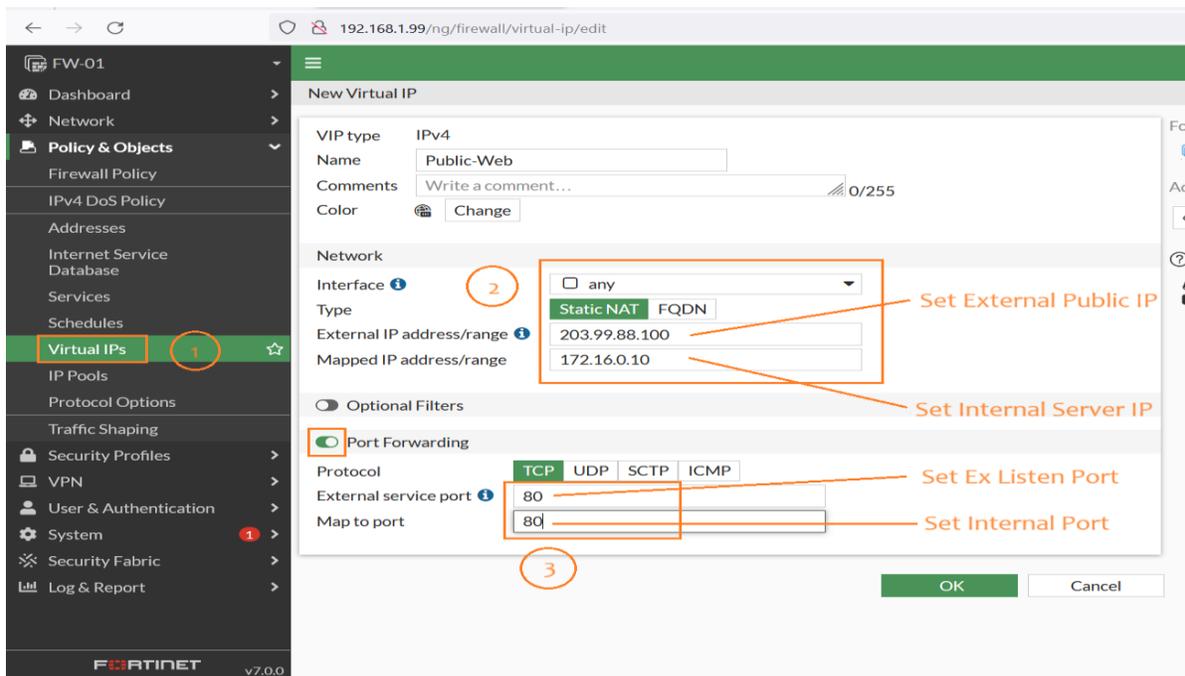
LAN To WAN Policy Ready

Security Rating Issues

## 7. Create “Virtual IP”



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



## Create Port Forwarding Firewall Policy For “Public

192.168.1.99/ng/firewall/policy/policy/standard/edit

New Policy

Name: PF-Web

Incoming Interface: WAN (port2)

Outgoing Interface: Service

Source: all

Destination: Public-Web

Schedule: always

Service: ALL\_ICMP, HTTP, HTTPS

Action: ACCEPT, DENY

Inspection Mode: Flow-based, Proxy-based

Firewall / Network Options

NAT:

IP Pool Configuration: Use Outgoing Interface Address, Use Dynamic IP Pool

Preserve Source Port:

Protocol Options: PROXY default

Security Profiles

Antivirus:

Web Filter:

DNS Filter:

Application Control:

IPS:

File Filter:

SSL Inspection: SSL no-inspection

Logging Options

Log Allowed Traffic:  Security Events All Sessions

Generate Logs when Session Starts:

Capture Packets:

Comments: Write a comment... 0/1023

Enable this policy:

OK Cancel

## Policy Ready For “WAN-To-LAN” DNAT

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
PF-Web	WAN (port2)	Service	all	Public-Web	always	ALL_ICMP, HTTP, HTTPS	ACCEPT	Enabled	SSL no-inspection	All	0B
LAN-To-WAN	Service	WAN (port2)	Service address	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	All	0B
Implicit Deny	any	any	all	all	always	ALL	DENY			Enabled	0B

## 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"

```
Public-Web
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 172.16.0.1 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.0.1
C 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
L 172.16.0.0/24 is directly connected, Ethernet0/0
L 172.16.0.10/32 is directly connected, Ethernet0/0

WEB#
WEB#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
..!!!.
Success rate is 40 percent (2/5), round-trip min/avg/max = 69/80/92 ms
WEB#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 69/11/82 ms
WEB#
```

## Check Logging From “LAN-172.16.0.10” To “8.8.8.8”

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
2024/05/18 08:28:09	172.16.0.10	aa:bb:cc:00:30:00	8.8.8.8 (dns.google)		✓ 500 B / 384 B	LAN-To-WAN (1)
2024/05/18 08:27:53	172.16.0.10	aa:bb:cc:00:30:00	8.8.8.8 (dns.google)		✓ 500 B / 384 B	LAN-To-WAN (1)
2024/05/18 08:27:33	172.16.0.10	aa:bb:cc:00:30:00	8.8.8.8 (dns.google)		✓ 2.00 kB / 1.82 kB	LAN-To-WAN (1)
2024/05/18 08:25:46	172.16.0.10	aa:bb:cc:00:30:00	8.8.8.8 (dns.google)		✓ 500 B / 480 B	LAN-To-WAN (1)
2024/05/18 08:25:06	203.99.88.1		203.99.88.100		✓ 527 B / 341 B	PF-Web (2)
2024/05/18 08:25:03	203.99.88.1		203.99.88.100		✓ 574 B / 396 B	PF-Web (2)
2024/05/18 08:16:03	203.99.88.1		203.99.88.100		✓ 260 B / 400 B	PF-Web (2)
2024/05/18 08:16:03	203.99.88.1		203.99.88.100		✓	PF-Web (2)
2024/05/18 08:16:02	203.99.88.1		203.99.88.100		✓	PF-Web (2)
2024/05/18 08:15:41	203.99.88.1		203.99.88.100		✓ 260 B / 320 B	PF-Web (2)
2024/05/18 08:15:41	203.99.88.1		203.99.88.100		✓	PF-Web (2)
2024/05/18 08:15:41	203.99.88.1		203.99.88.100		✓ 260 B / 320 B	PF-Web (2)
2024/05/18 08:15:41	203.99.88.1		203.99.88.100		✓ 260 B / 320 B	PF-Web (2)
2024/05/18 08:15:41	203.99.88.1		203.99.88.100		✓	PF-Web (2)
2024/05/18 08:15:34	203.99.88.1		203.99.88.100		✓ 260 B / 320 B	PF-Web (2)
2024/05/18 08:15:34	203.99.88.1		203.99.88.100		✓	PF-Web (2)
2024/05/18 08:15:23	203.99.88.1		203.99.88.100		✓ 156 B / 240 B	PF-Web (2)
2024/05/18 08:15:23	203.99.88.1		203.99.88.100		✓	PF-Web (2)
2024/05/18 08:15:22	203.99.88.1		203.99.88.100		✓ 156 B / 240 B	PF-Web (2)

## Check Public Web Server Access From “Public”

### Check Lan IP

```

C:\Windows\system32\cmd.e. X + v
Connection-specific DNS Suffix . :
Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . :
Link-Local IPv6 Address . . . . . : fe80::157b:a3bd:c04b:b902%25
IPv4 Address. . . . . : 192.168.1.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . :
Link-Local IPv6 Address . . . . . : fe80::ac20:cf35:bb43:dced%9
IPv4 Address. . . . . : 203.99.88.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter Ethernet 2:

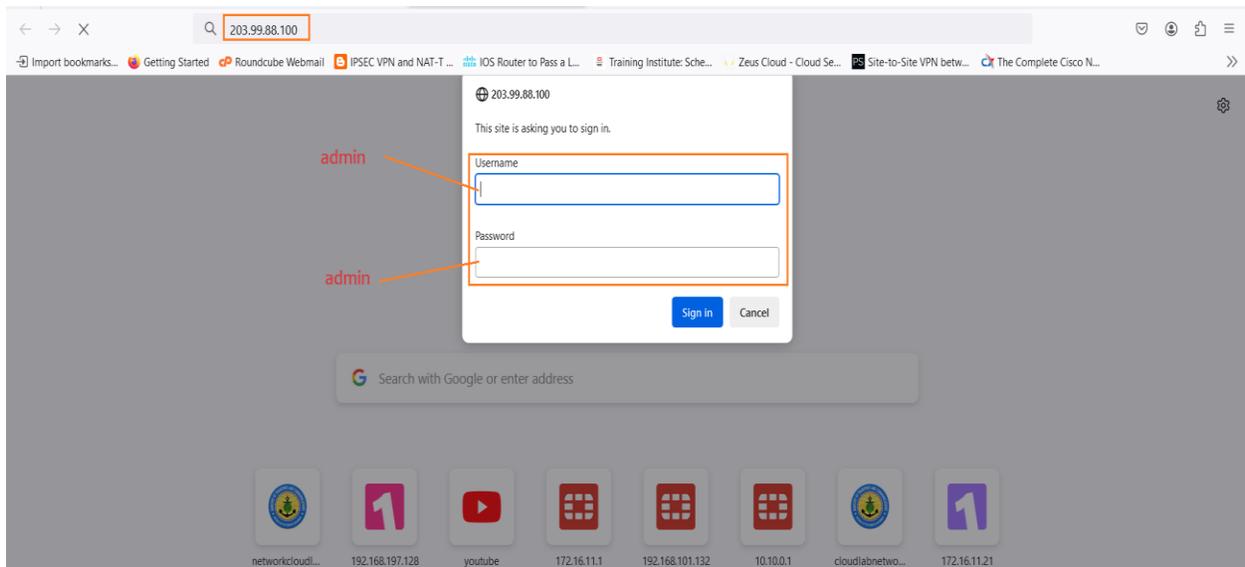
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 6:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:
    
```

## Browse to Public IP ( WAN IP )



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

