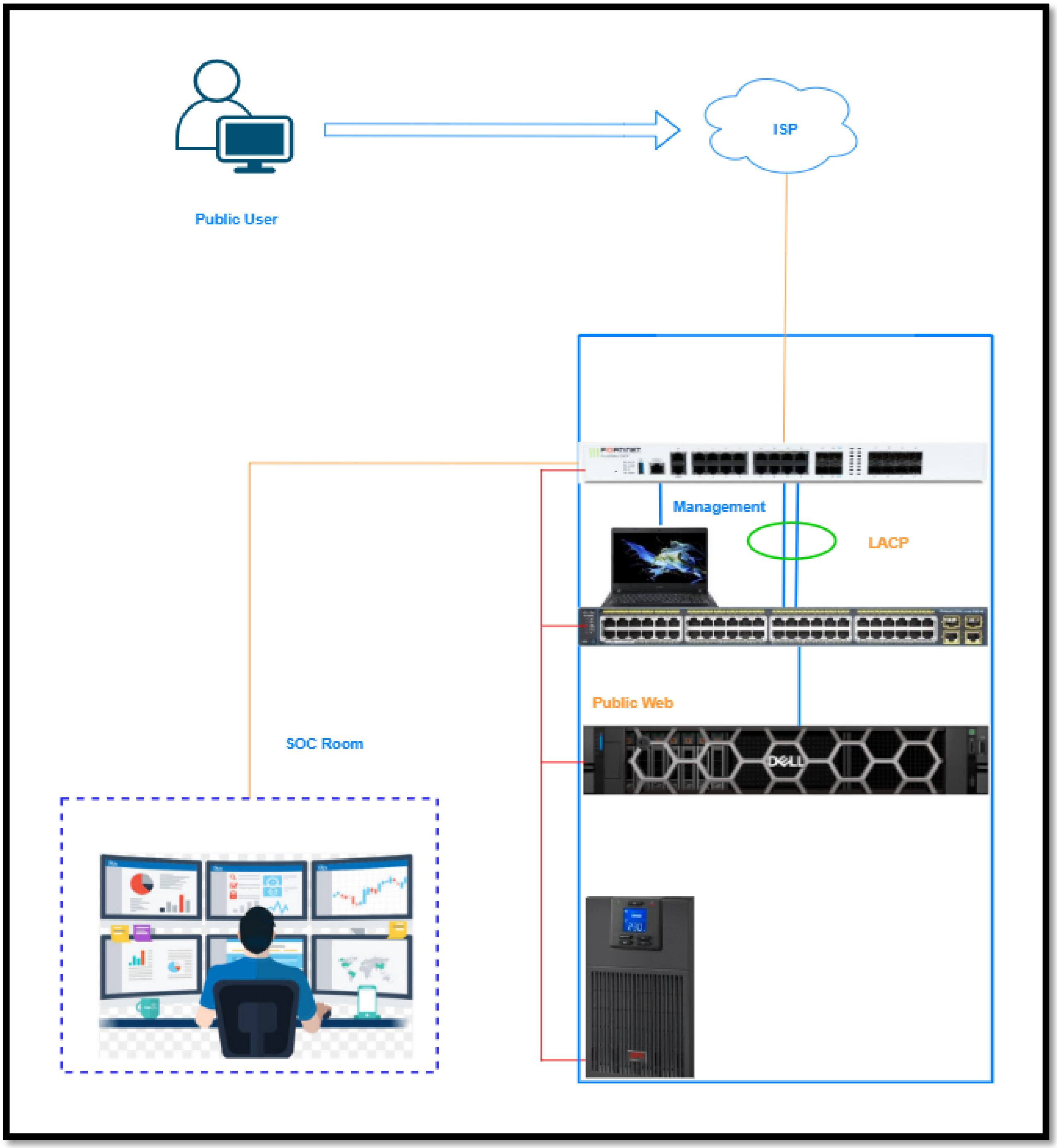
FortiGate Configuration

(Mini DC Project)



Job Requirements

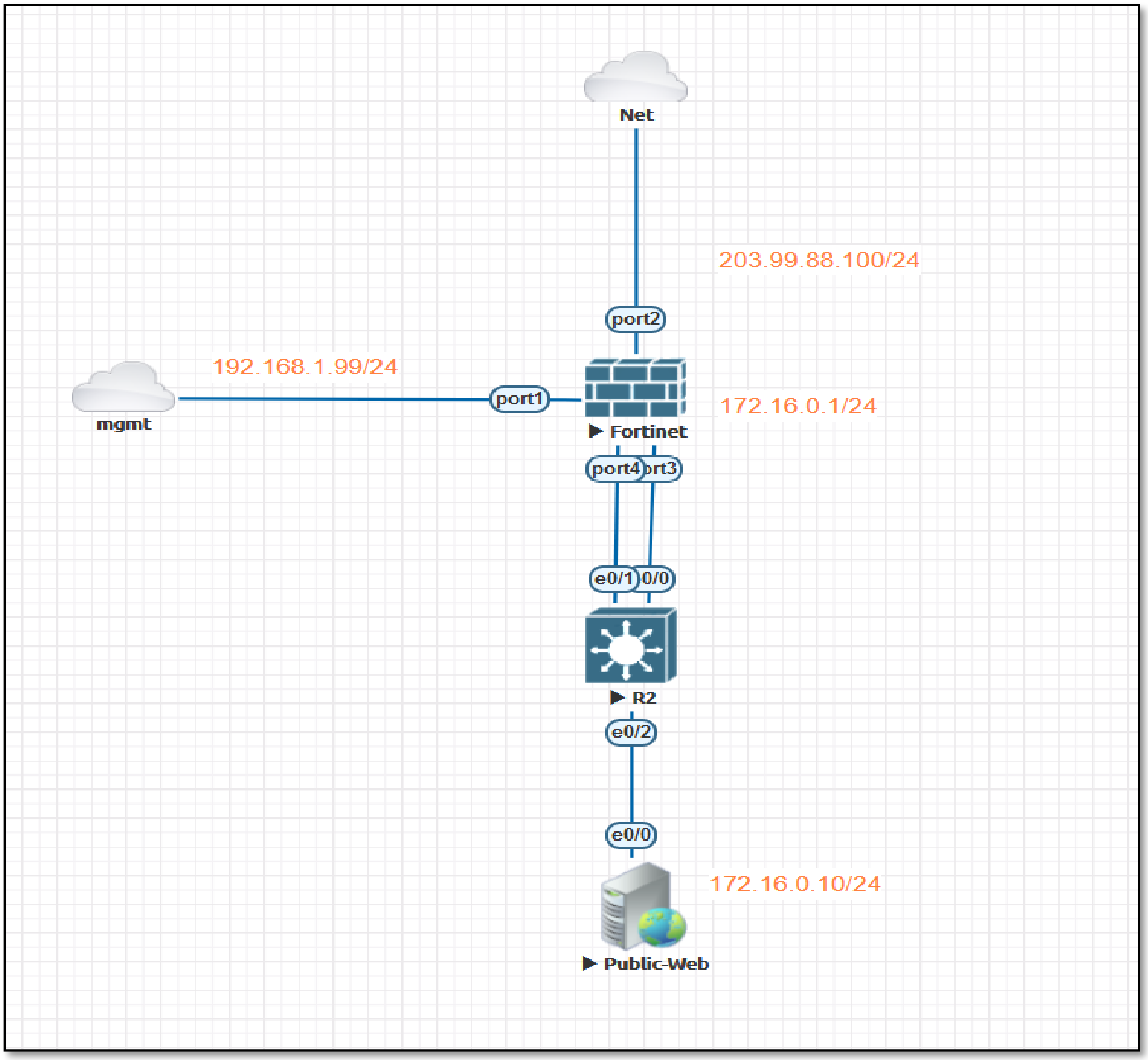
Customer have 1 Dell server, 1 Cisco Catalyst Switch, 1 FortiGate 200F Firewall. Customer want to use Secure LAN network for Internet Access and also want to public their private web-Server.

Service Component

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

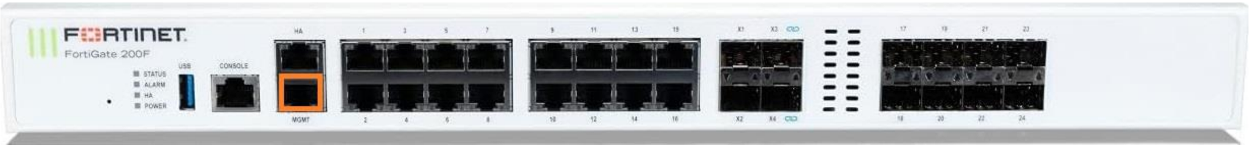
IP Address List

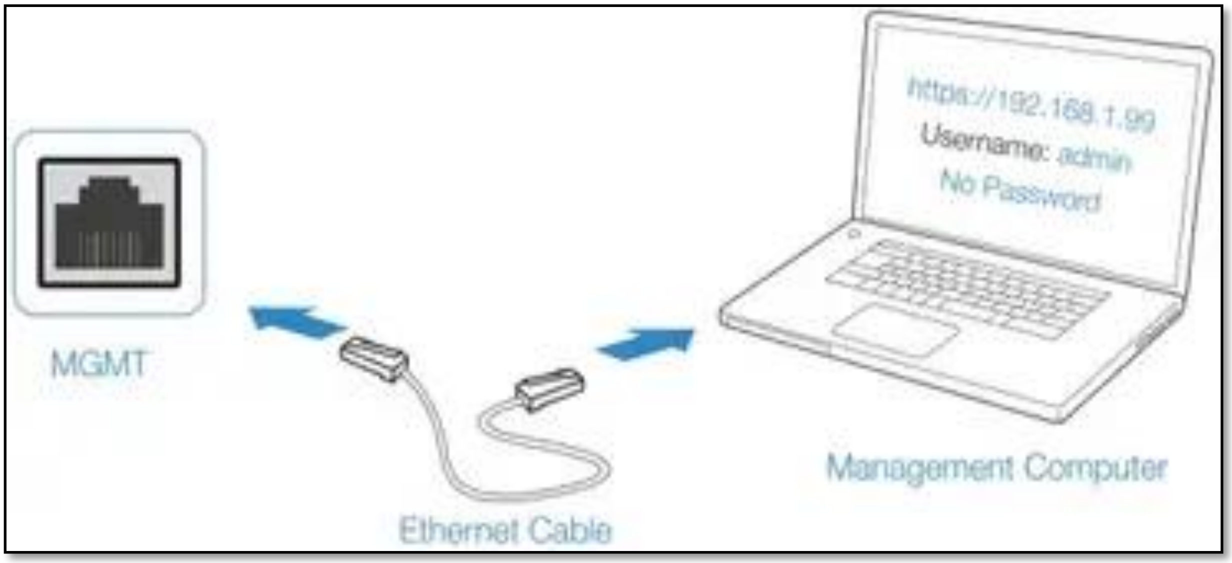
No	Zone Name	IP Address	Gateway	Remark
1	WAN	203.99.88.100/24	203.99.88.2	
2	Mgmt	192.168.1.99/24		
3	LACP			Port 3-4
4	Service	172.16.0.1/24	172.16.0.1	VLAN
5	Web-Server	172.16.0.10/24	172.16.0.1	



1. Initial Configuration

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

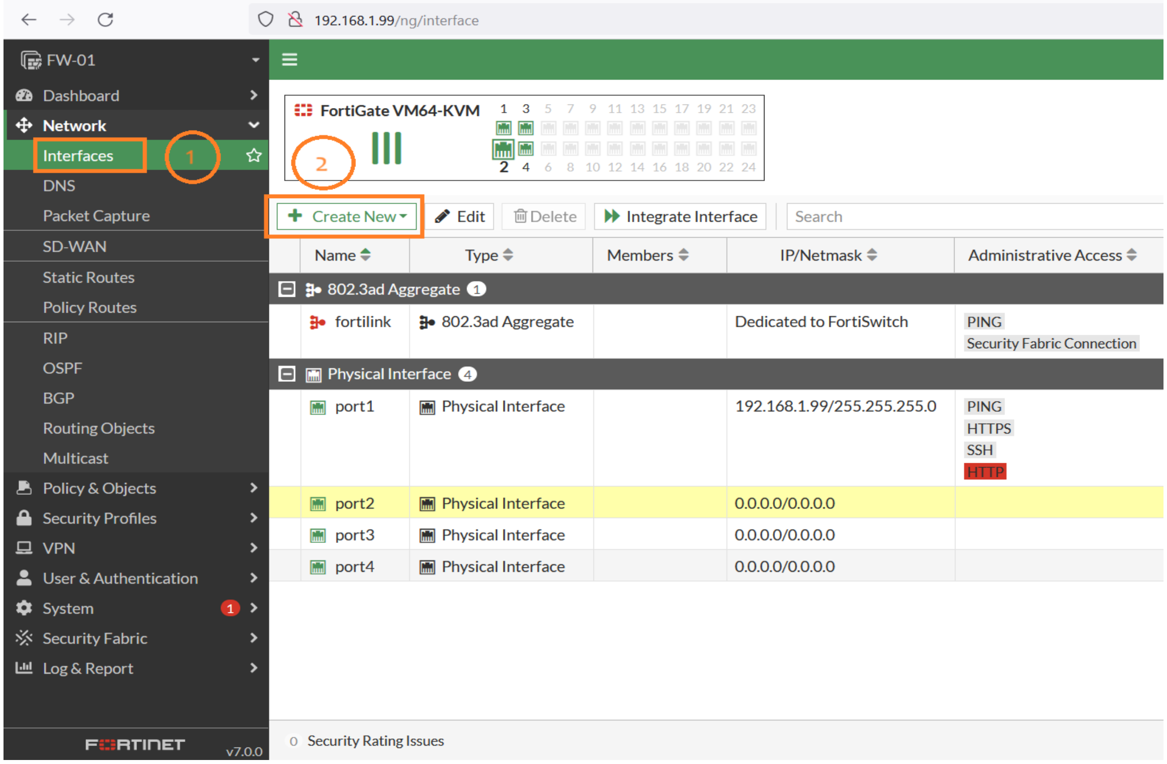




Manual Configuration [via Console]

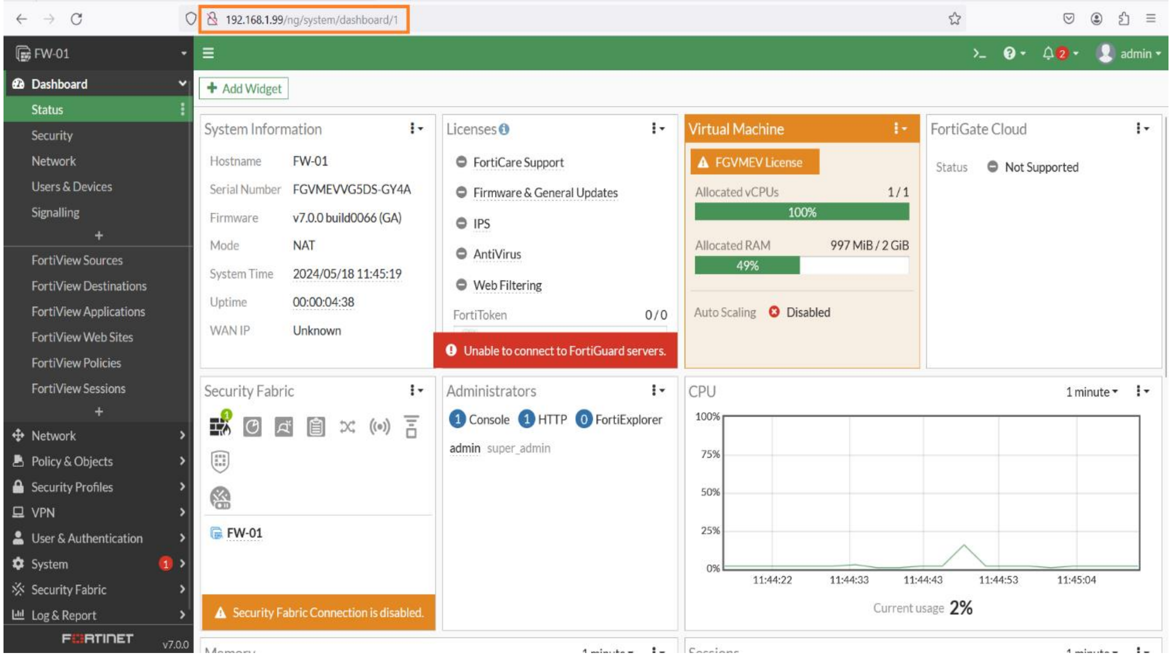
```
FortiGate-VM64-KVM # config system interface

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
802.3ad Aggregate 1				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
Physical Interface 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 FGVMEVVG5DS-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

Unable to connect to FortiGuard servers.

Virtual Machine

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

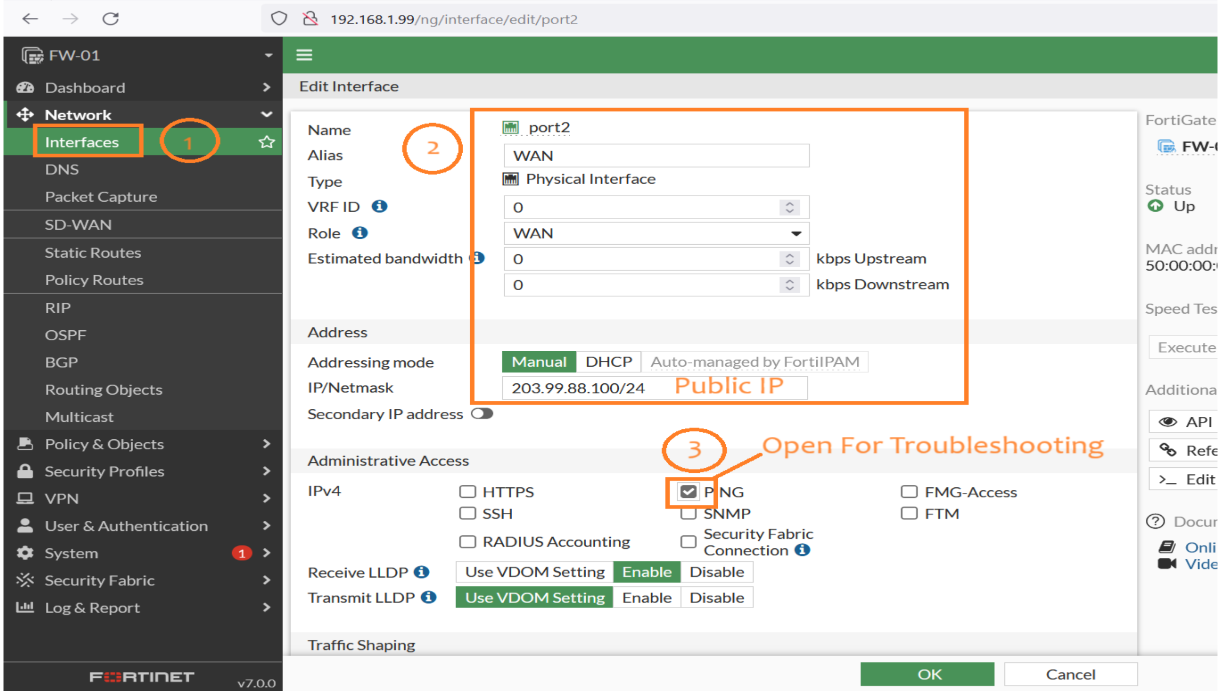
FortiGate Cloud

Status Not Supported

Security Fabric Connection is disabled.

1 Console 1 HTTP 0 FortiExplorer
admin super_admin

Current usage 2%



Edit Interface

Name	port2
Alias	WAN
Type	Physical Interface
VRF ID	0
Role	WAN
Estimated bandwidth	0 kbps Upstream 0 kbps Downstream

Address

Addressing mode	[✓ Manual] DHCP Auto-managed by FortiIPAM
IP/Netmask	203.99.88.100/24
Secondary IP address	○

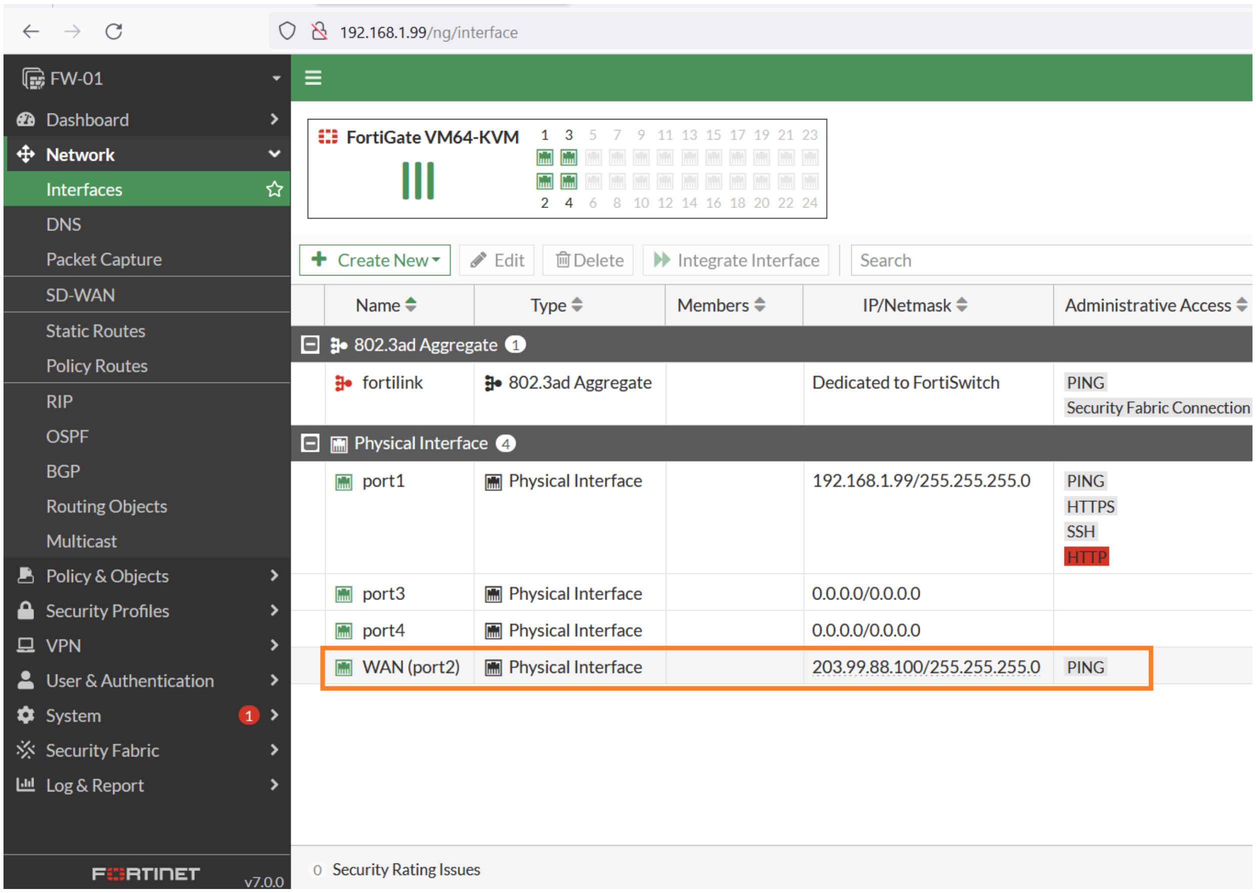
Administrative Access

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

Receive LLDP	Use VDOM Setting [✓ Enable] Disable
Transmit LLDP	[✓ Use VDOM Setting] Enable Disable

Traffic Shaping

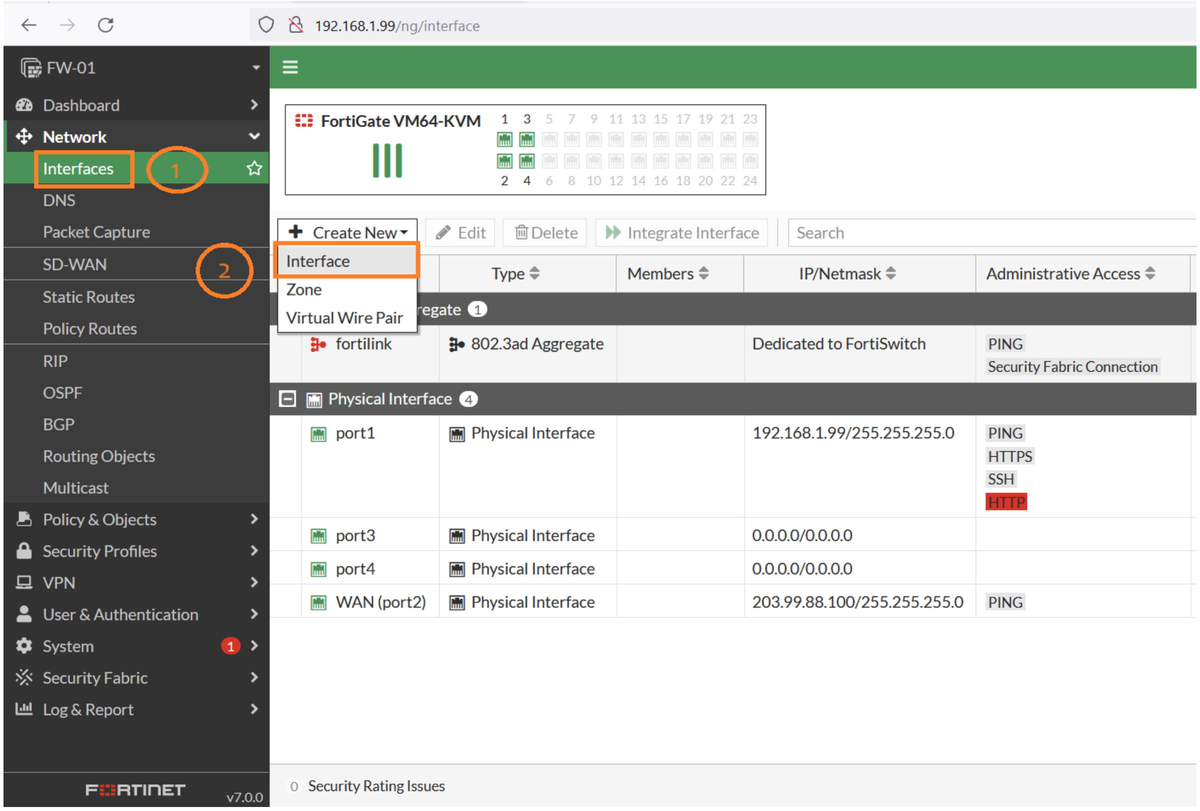
Interface Ready For “ WAN”



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

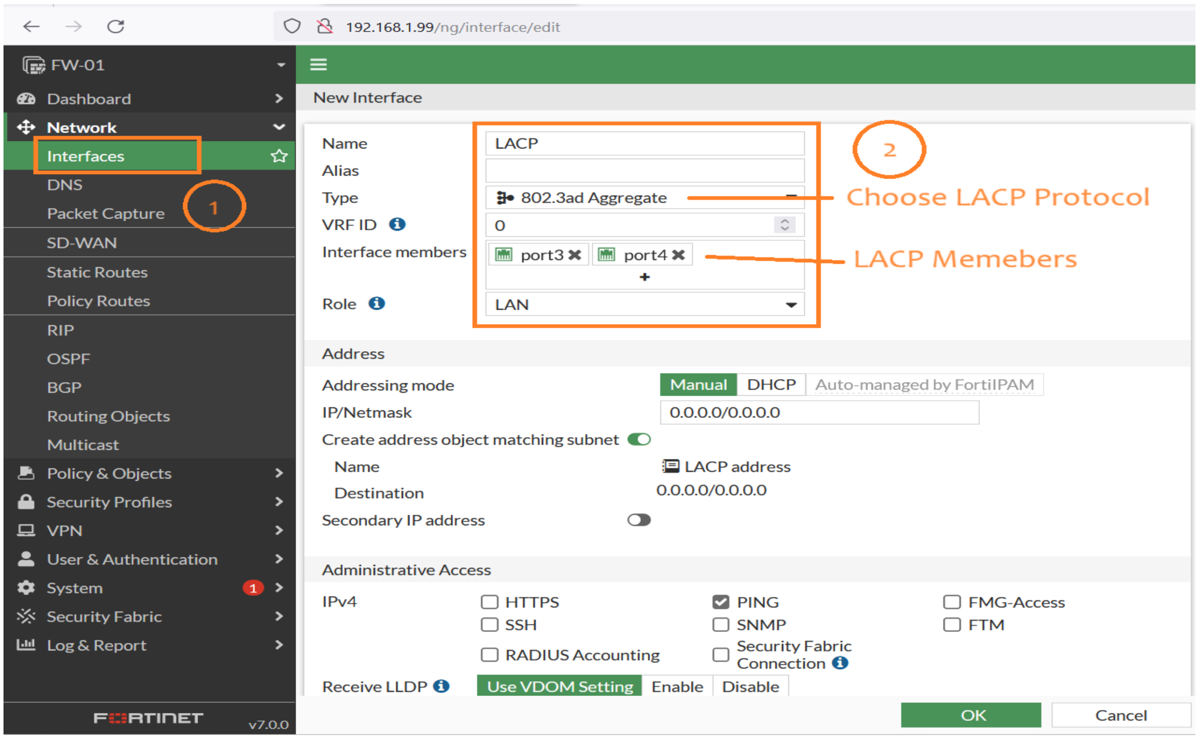
0 Security Rating Issues

4. Configure LAN interface



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

Configure “Aggregate Interface”



New Interface

Name: LACP

Alias:

Type: 802.3ad Aggregate

VRF ID: 0

Interface members: port3 ✖ port4 ✖ +

Role: LAN

Choose LACP Protocol

LACP Memebers

Address

Addressing mode: [✓ Manual] DHCP Auto-managed by FortiIPAM

IP/Netmask: 0.0.0.0/0.0.0.0

Create address object matching subnet ●

Name: LACP address

Destination: 0.0.0.0/0.0.0.0

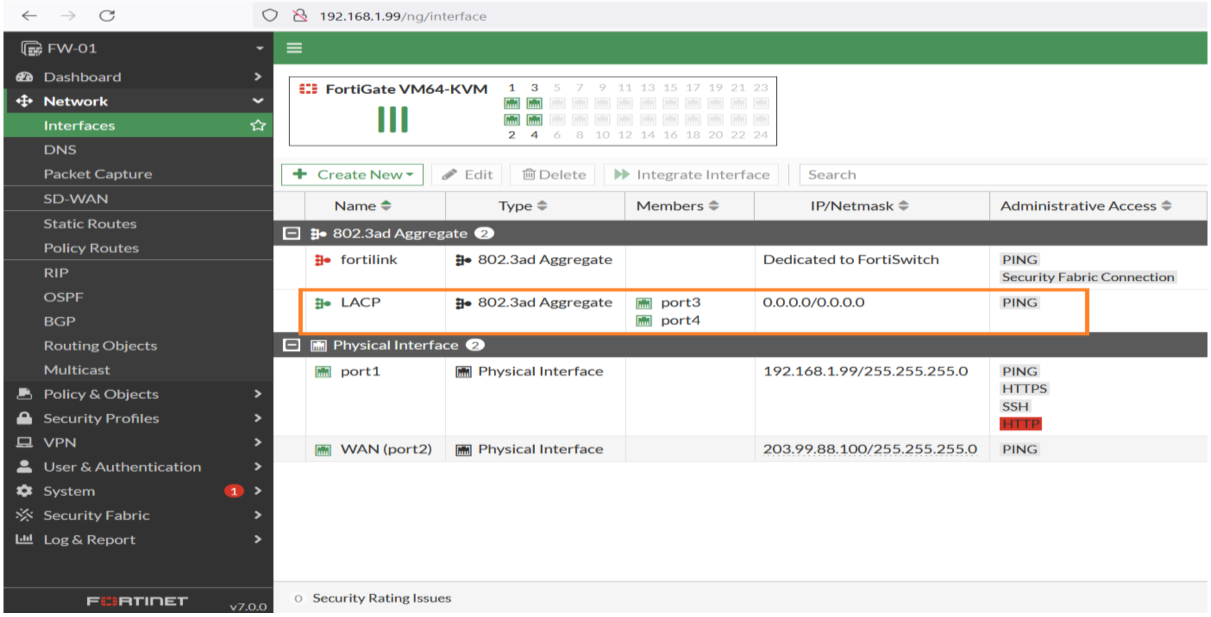
Secondary IP address ○

Administrative Access

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

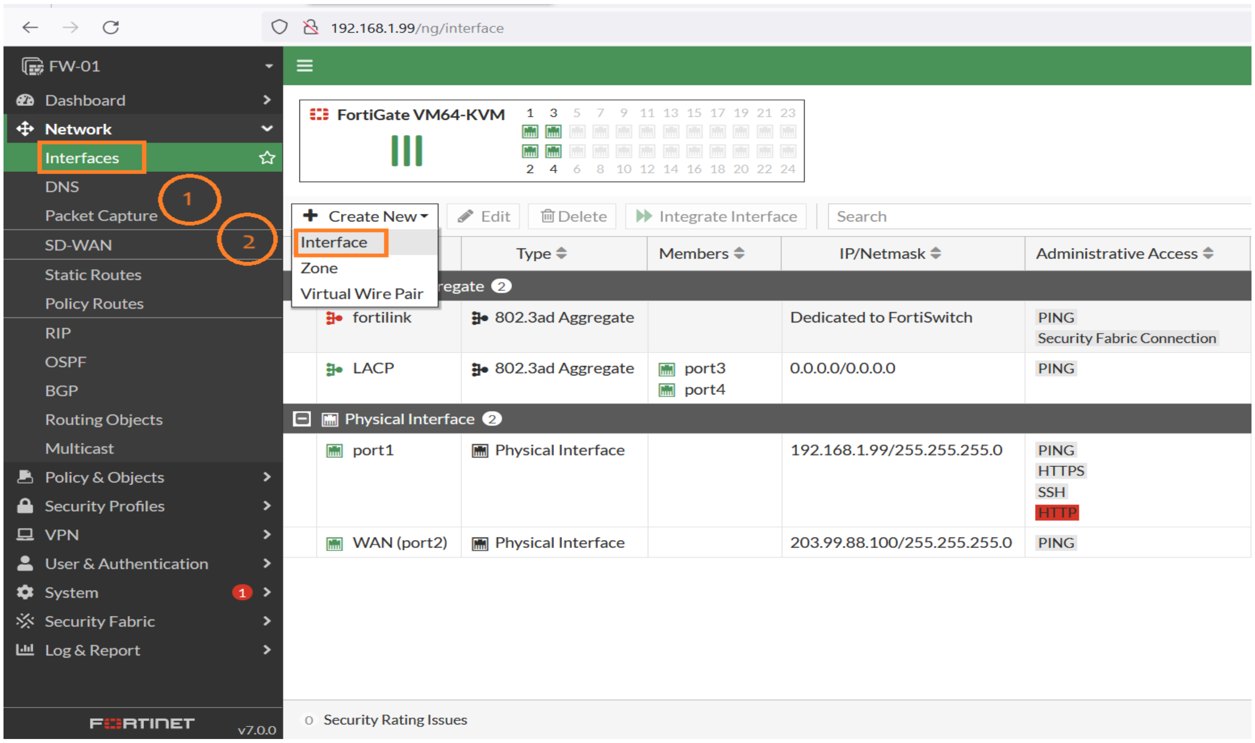
Receive LLDP: [✓ Use VDOM Setting] Enable Disable

“Aggreate” interface ready

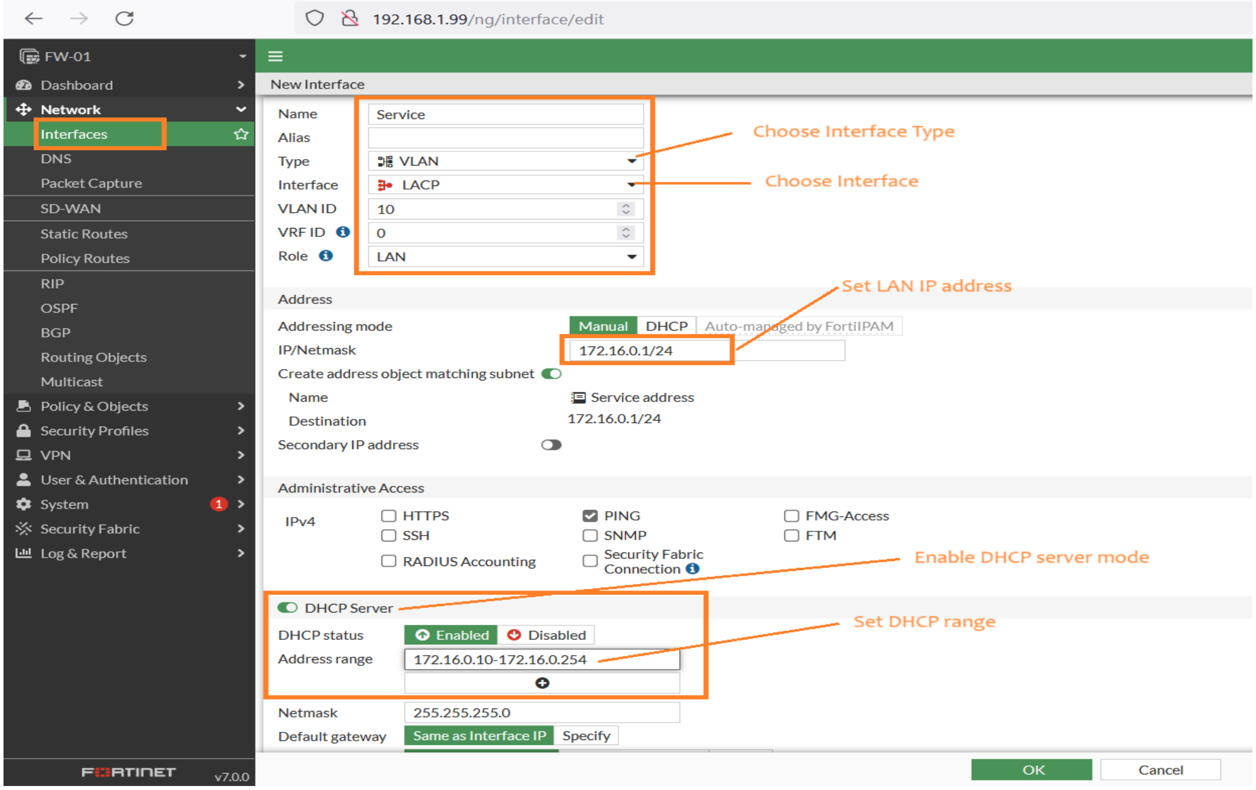


Name	Type	Members	IP/Netmask	Administrative Access
802.3ad Aggregate 2				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
LACP	802.3ad Aggregate	port3 port4	0.0.0.0/0.0.0.0	PING
Physical Interface 2				
port1	Physical Interface		192.168.1.99/255.255.255.0	PING HTTPS SSH HTTP
WAN (port2)	Physical Interface		203.99.88.100/255.255.255.0	PING

5. Create VLAN for Service Network



	Type	Members	IP/Netmask	Administrative Access
regate 2				
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
Physical Interface 2				
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



New Interface

Name: Service
Alias:
Type: VLAN
Interface: LACP
VLAN ID: 10
VRF ID: 0
Role: LAN

Choose Interface Type

Choose Interface

Set LAN IP address

Address

Addressing mode: Manual | DHCP | Auto-managed by FortiIPAM
IP/Netmask: 172.16.0.1/24
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

Enable DHCP server mode

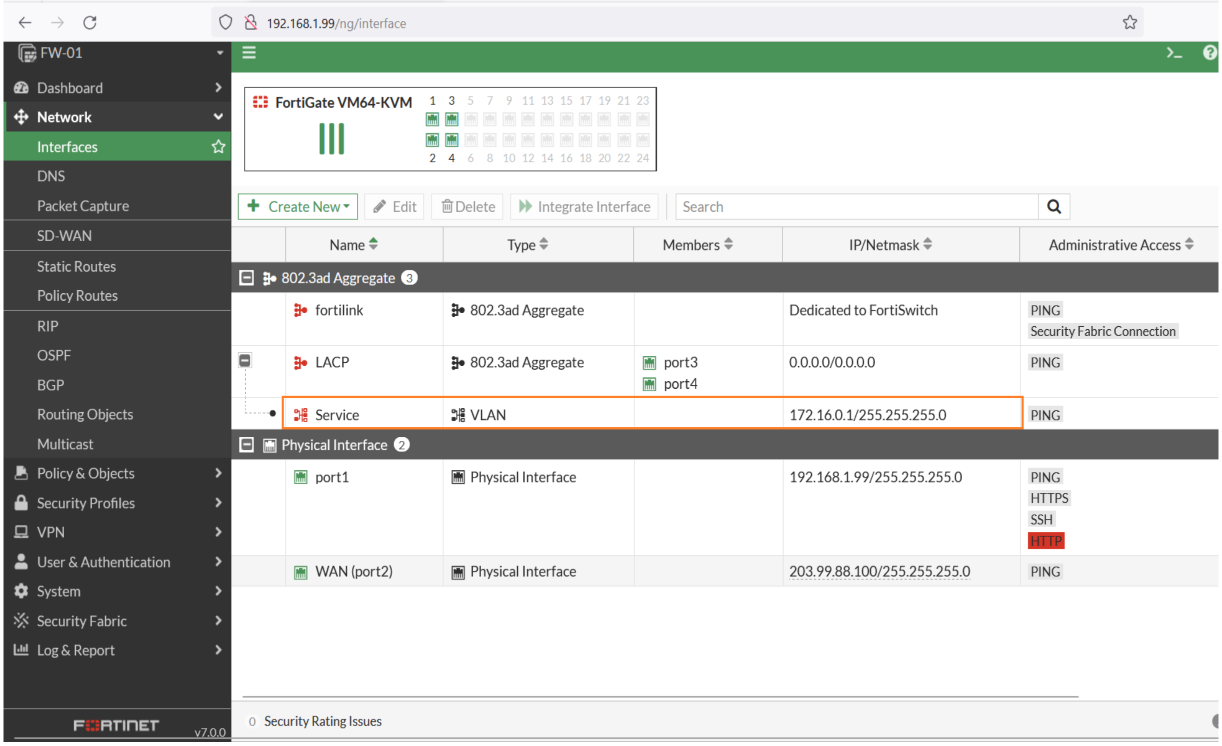
DHCP Server
DHCP status: Enabled | Disabled
Address range: 172.16.0.10-172.16.0.254

Set DHCP range

Netmask: 255.255.255.0
Default gateway: Same as Interface IP | Specify

OK   Cancel

Service VLAN Ready

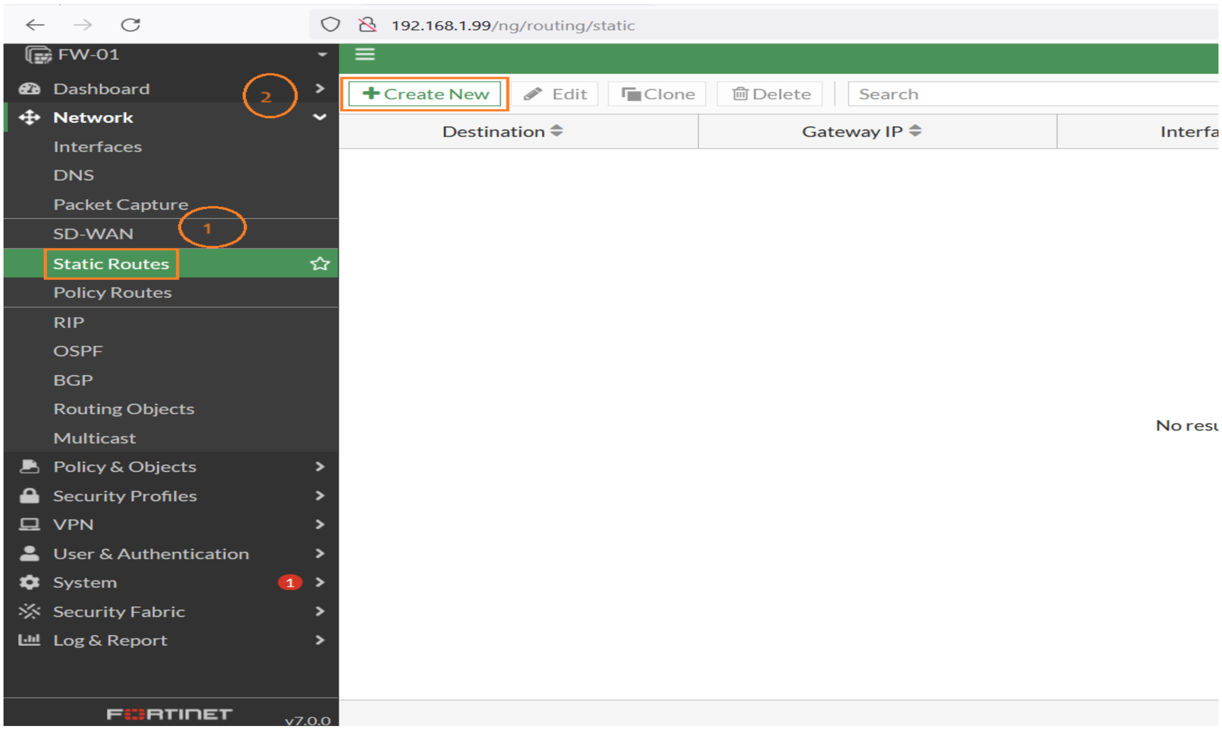


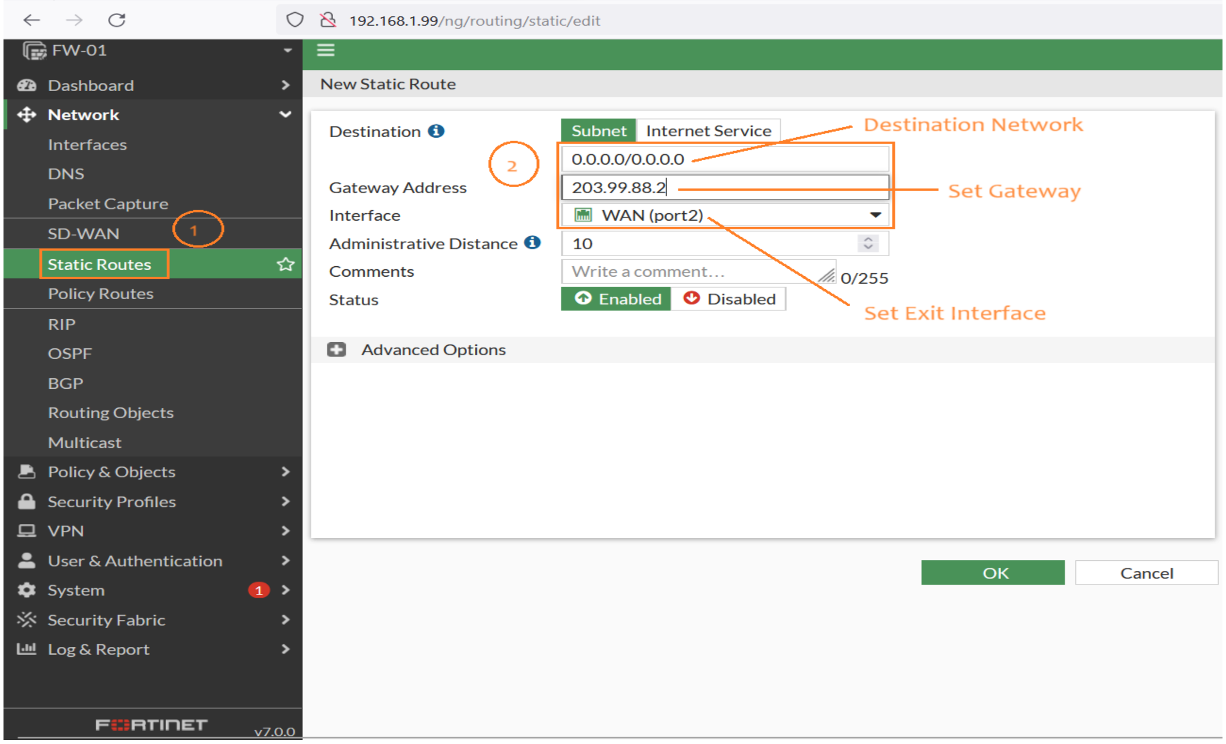
Name	Type	Members	IP/Netmask	Administrative Access
802.3ad Aggregate 3				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
LACP	802.3ad Aggregate	port3 port4	0.0.0.0/0.0.0.0	PING
Service	VLAN		172.16.0.1/255.255.255.0	PING
Physical Interface 2				
port1	Physical 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





New Static Route

Destination: Subnet | Internet Service — 0.0.0.0/0.0.0.0

Gateway Address: 203.99.88.2

Interface: WAN (port2)

Administrative Distance: 10

Comments: Write a comment... 0/255

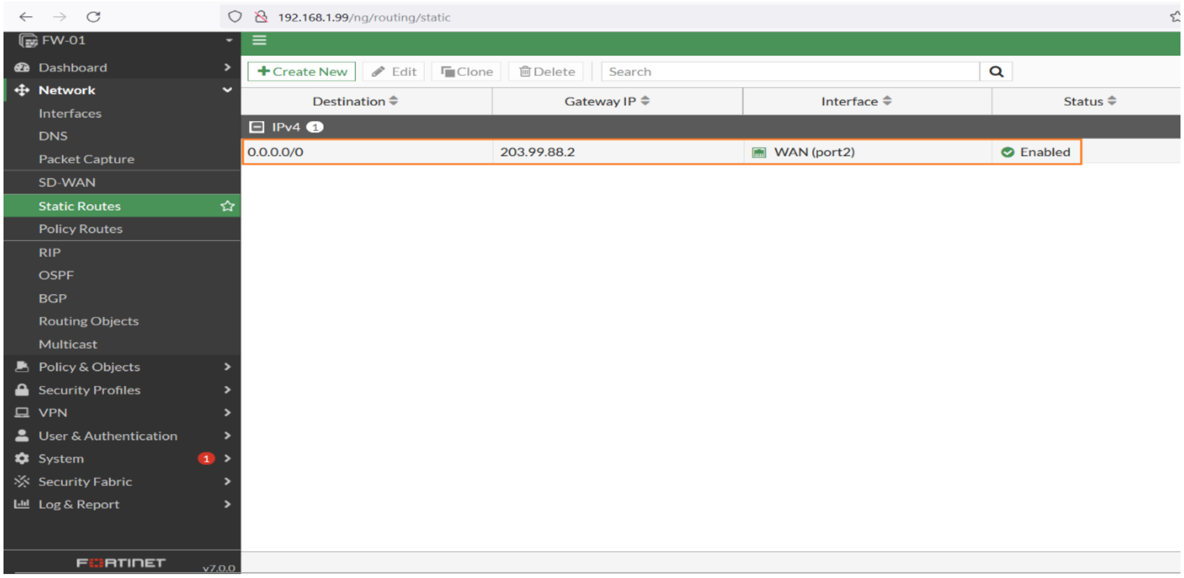
Status: Enabled | Disabled

Destination Network

Set Gateway

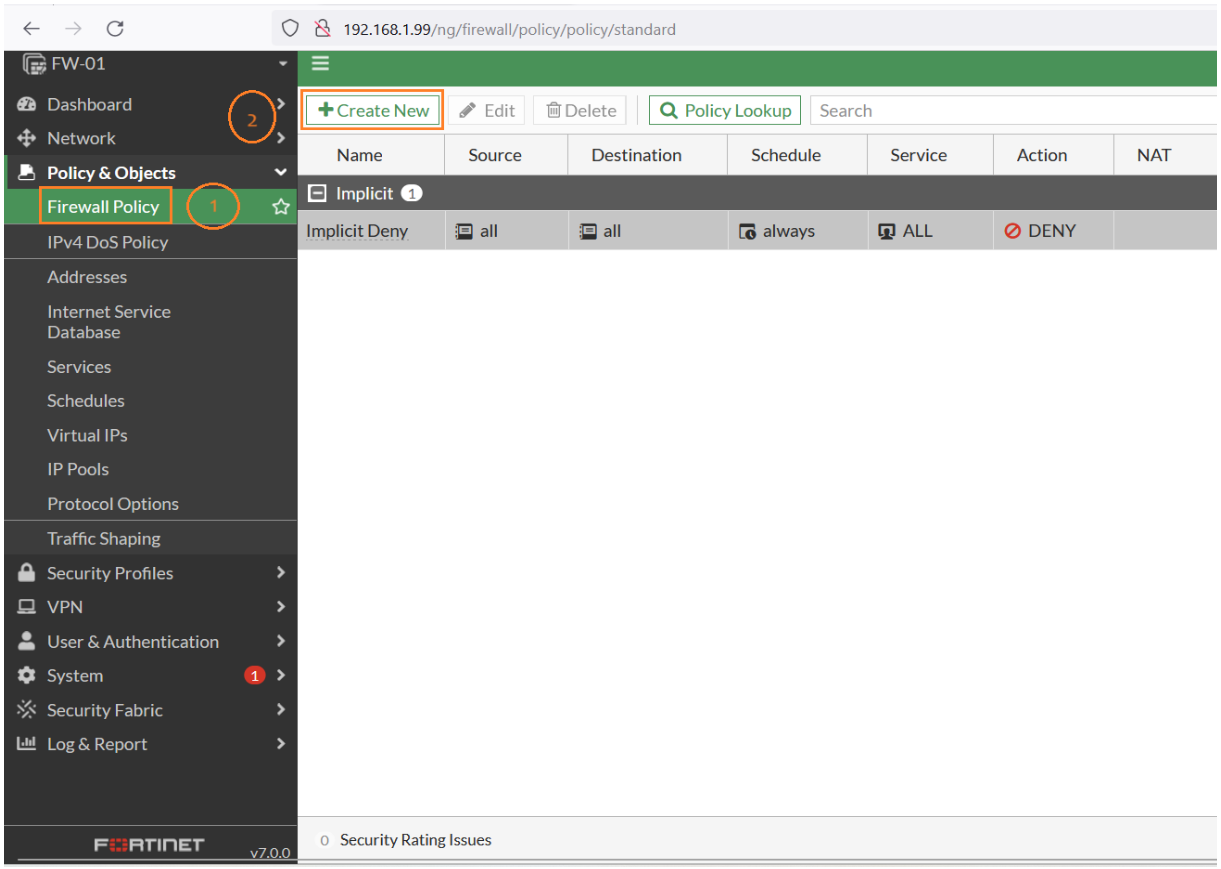
Set Exit Interface

Static Route Ready

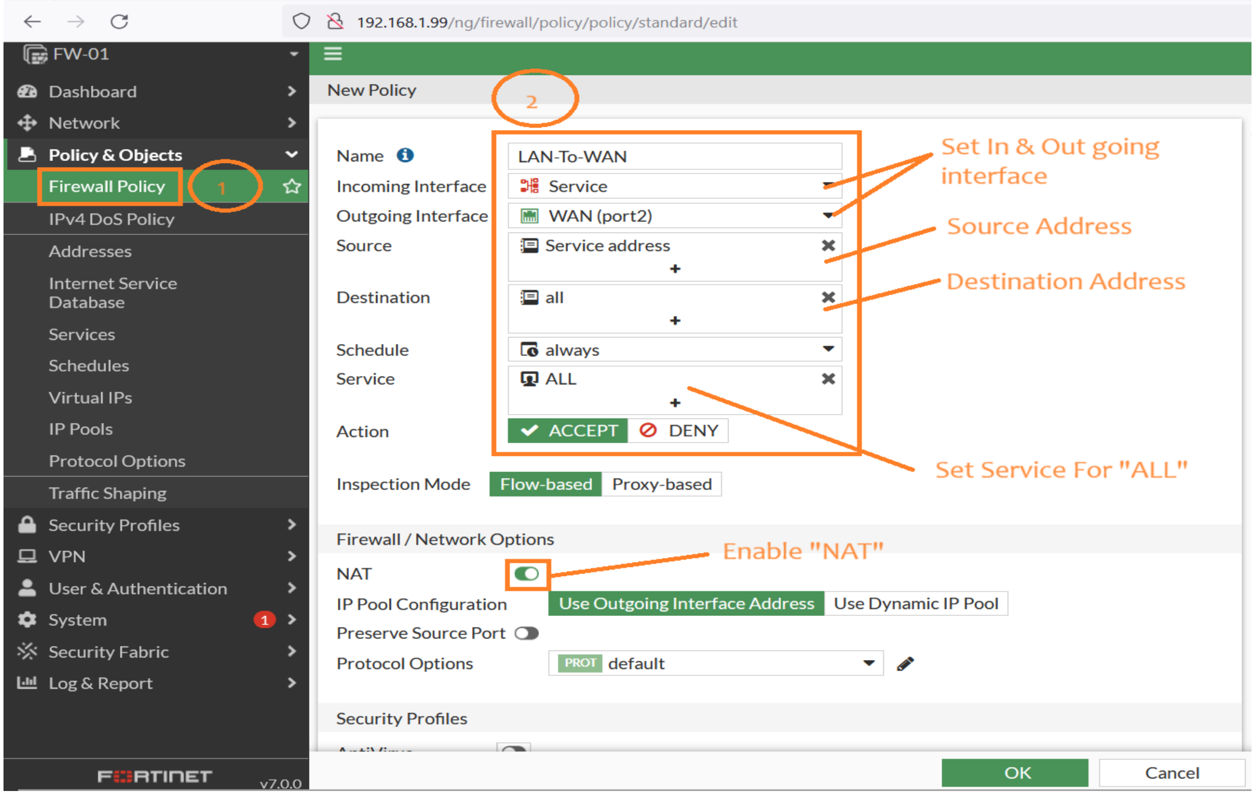


Destination	Gateway IP	Interface	Status
IPv4 1			
0.0.0.0/0	203.99.88.2	WAN (port2)	Enabled

Firewall Policy For “LAN-To-WAN”



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



New Policy

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

Firewall / Network Options

NAT: ●
IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool
Preserve Source Port: ○
Protocol Options: PROT default

Security Profiles

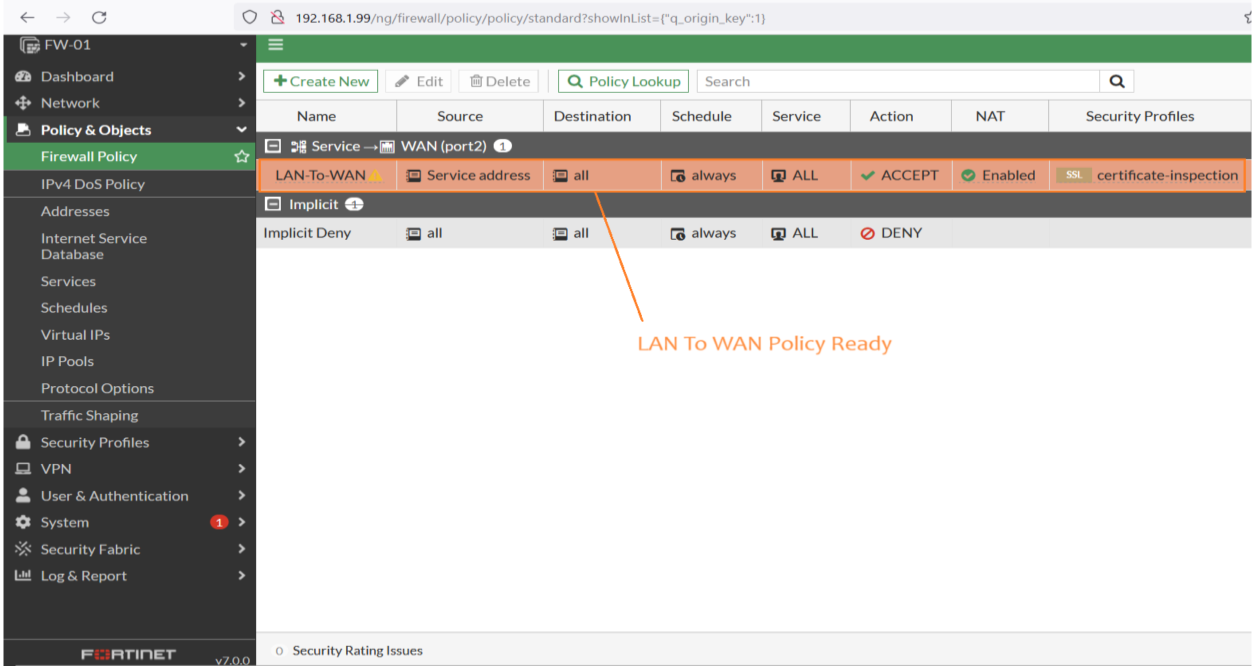
Set In & Out going interface

Source Address

Destination Address

Set Service For "ALL"

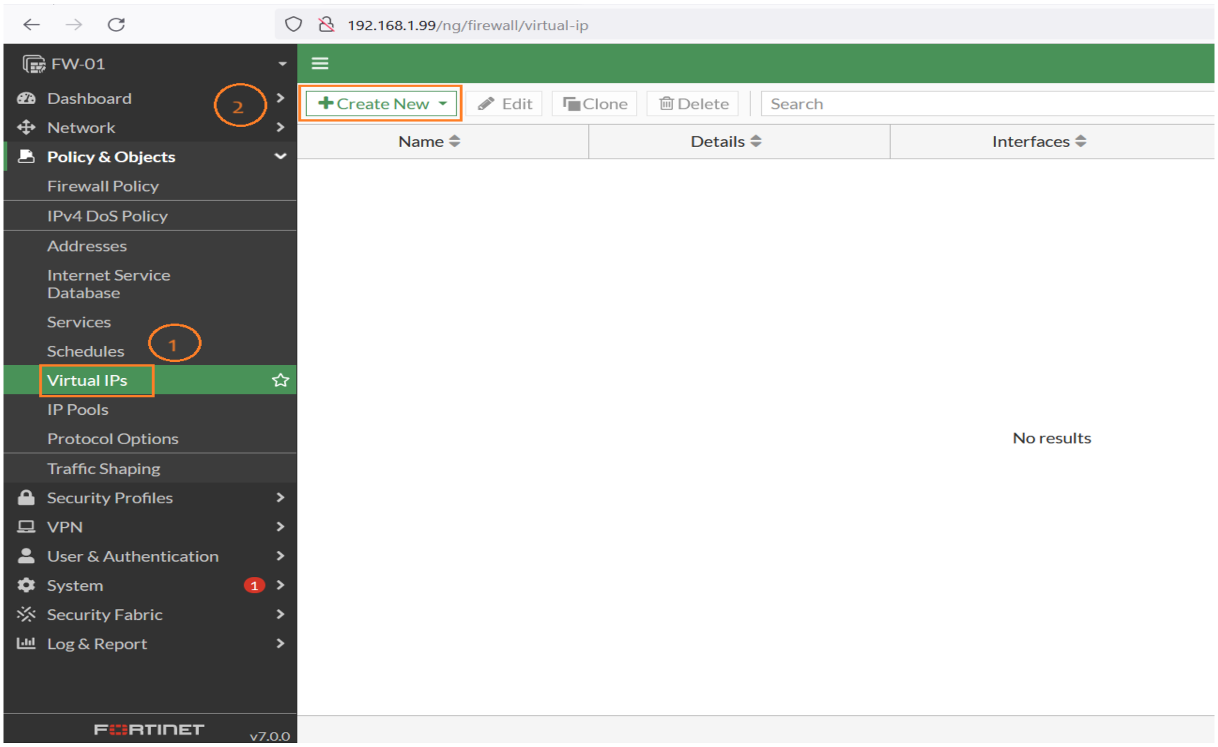
Enable "NAT"



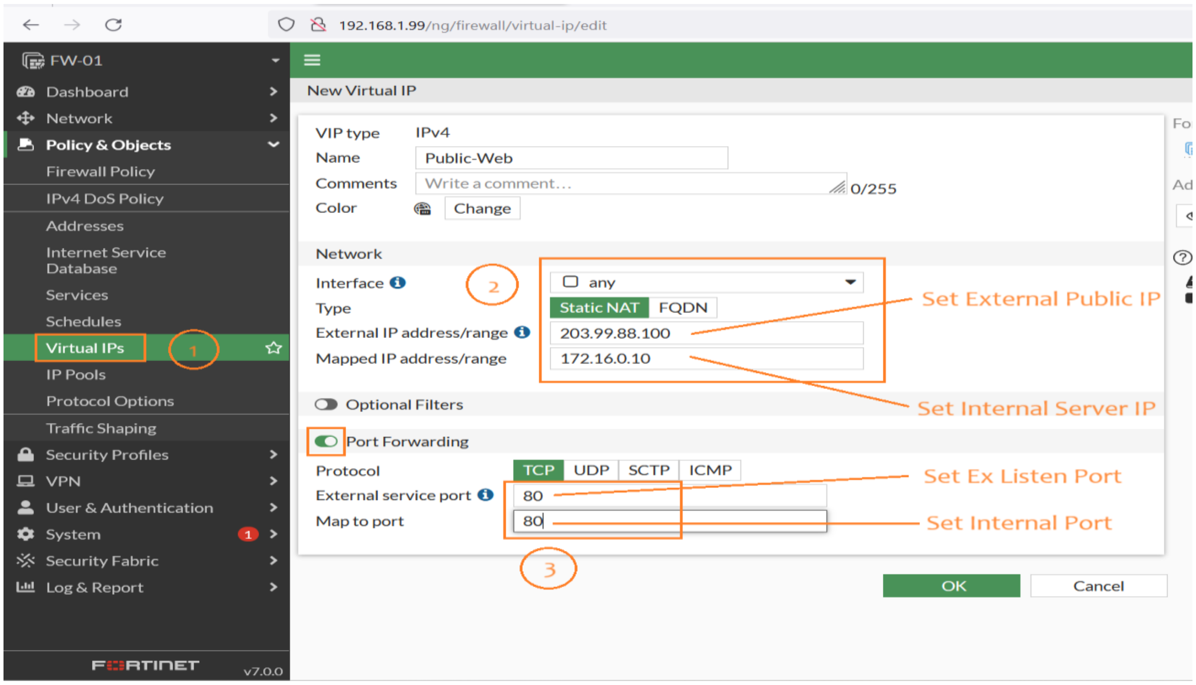
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
Service → WAN (port2) 1							
LAN-To-WAN	Service address	all	always	ALL	✓ ACCEPT	Enabled	SSL certificate-inspection
Implicit 1							
Implicit Deny	all	all	always	ALL	⊘ DENY		

LAN To WAN Policy Ready

7. Create “Virtual IP”



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



New Virtual IP

VIP type	IPv4
Name	Public-Web
Comments	Write a comment... 0/255
Color	Change

Network

Interface	any
Type	Static NAT / FQDN
External IP address/range	203.99.88.100
Mapped IP address/range	172.16.0.10

Optional Filters

Port Forwarding

Protocol	TCP / UDP / SCTP / ICMP
External service port	80
Map to port	80

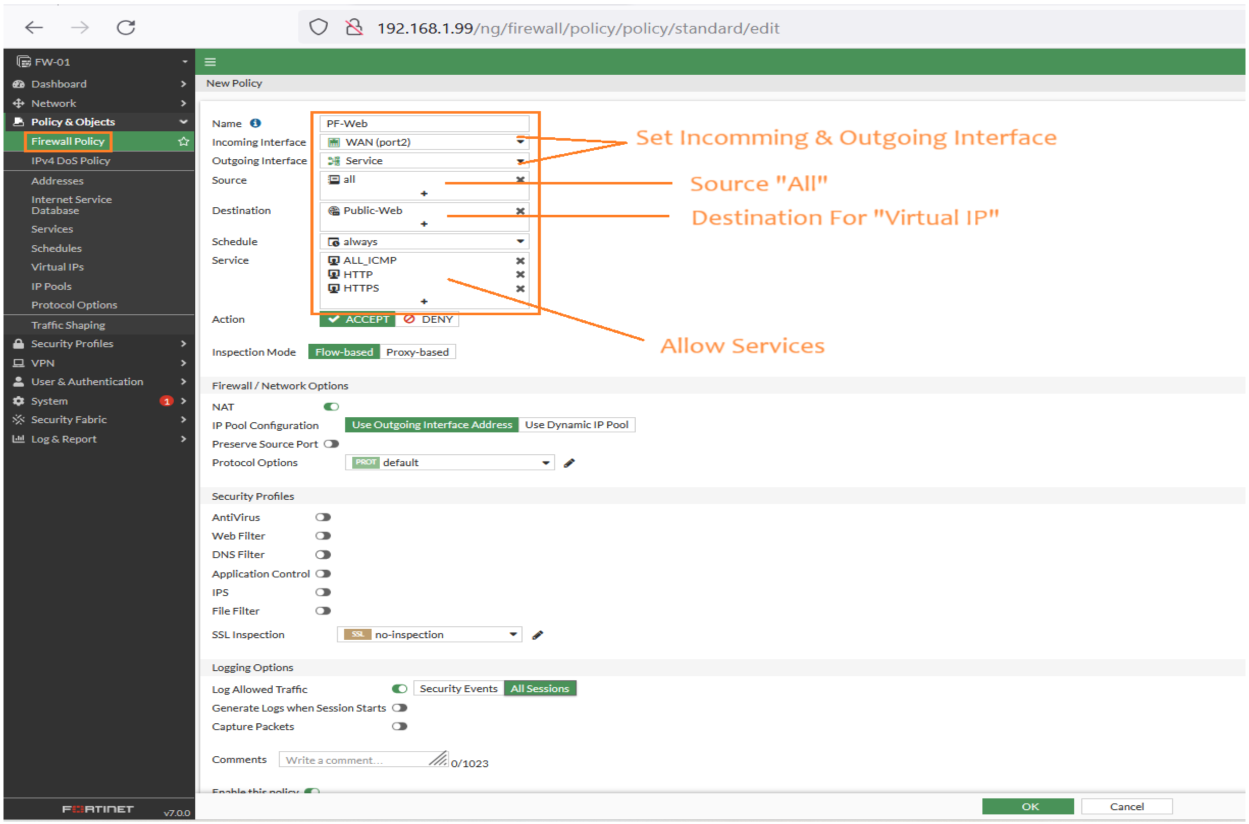
Set External Public IP

Set Internal Server IP

Set Ex Listen Port

Set Internal Port

Create Port Forwarding Firewall Policy For “Public



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: PROT 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 ●

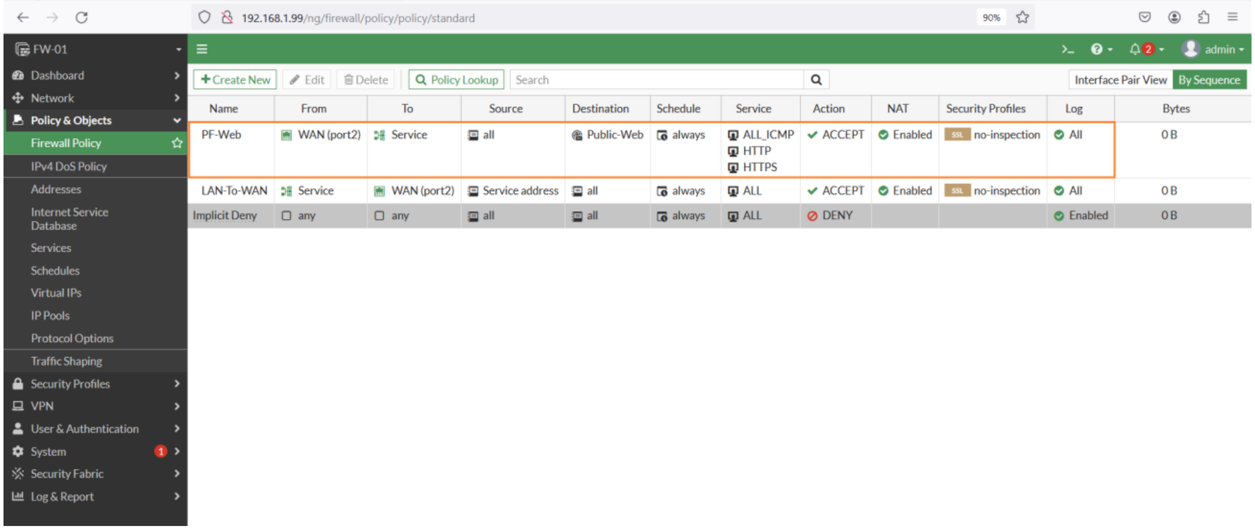
Set Incomming & Outgoing Interface

Source "All"

Destination For "Virtual IP"

Allow Services

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	0 B
LAN-To-WAN	Service	WAN (port2)	Service address	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	All	0 B
Implicit Deny	any	any	all	all	always	ALL	DENY			Enabled	0 B

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
------+-------------+-----------+-----------------------------------------------
```

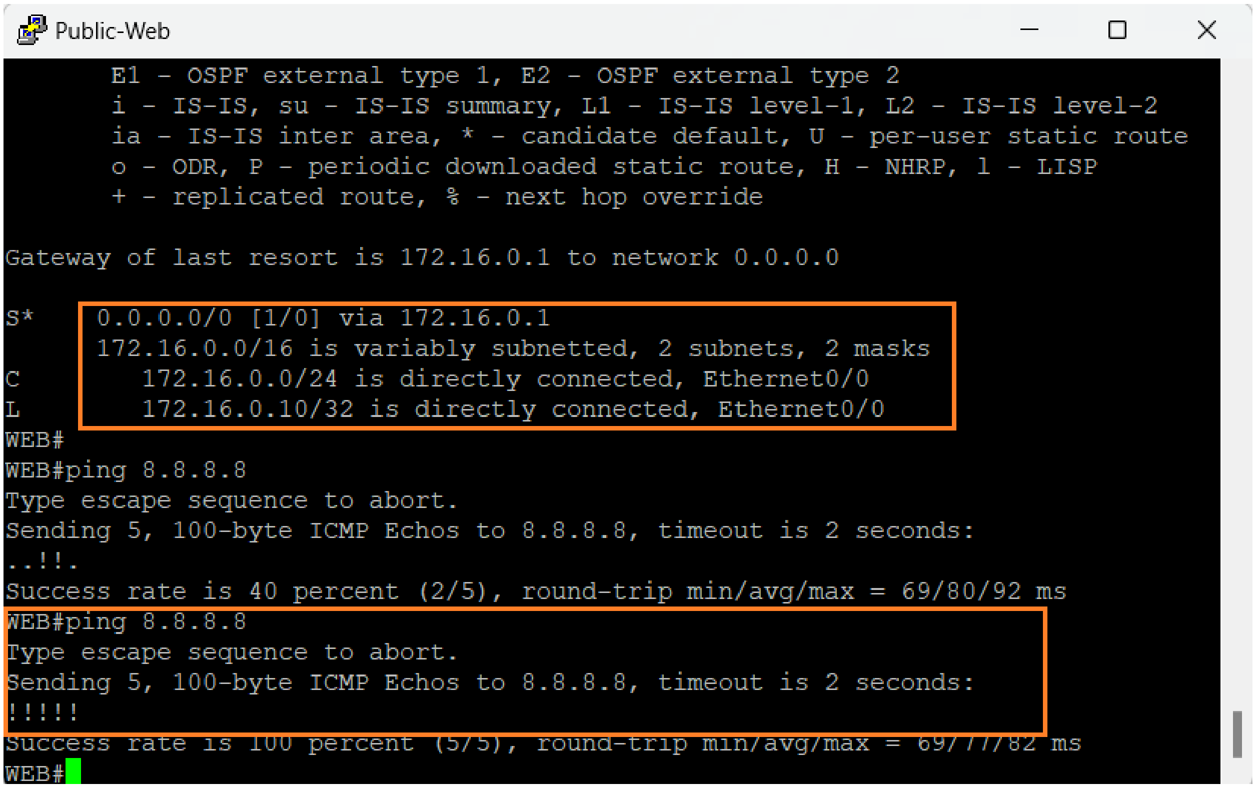
```
10     Po10(SU)       LACP     Et0/0(P)    Et0/1(P)
```

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
```

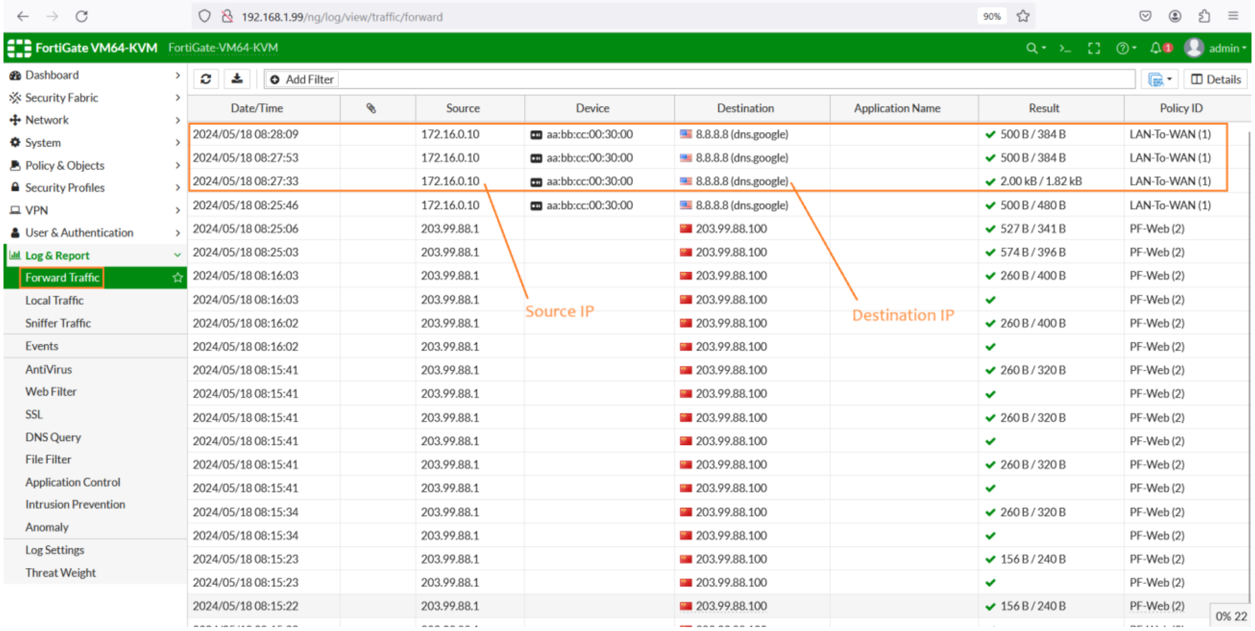
Service Testing

Ping Test From "LAN" to "8.8.8.8"



```
       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
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        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 = 69/77/82 ms
WEB#
```

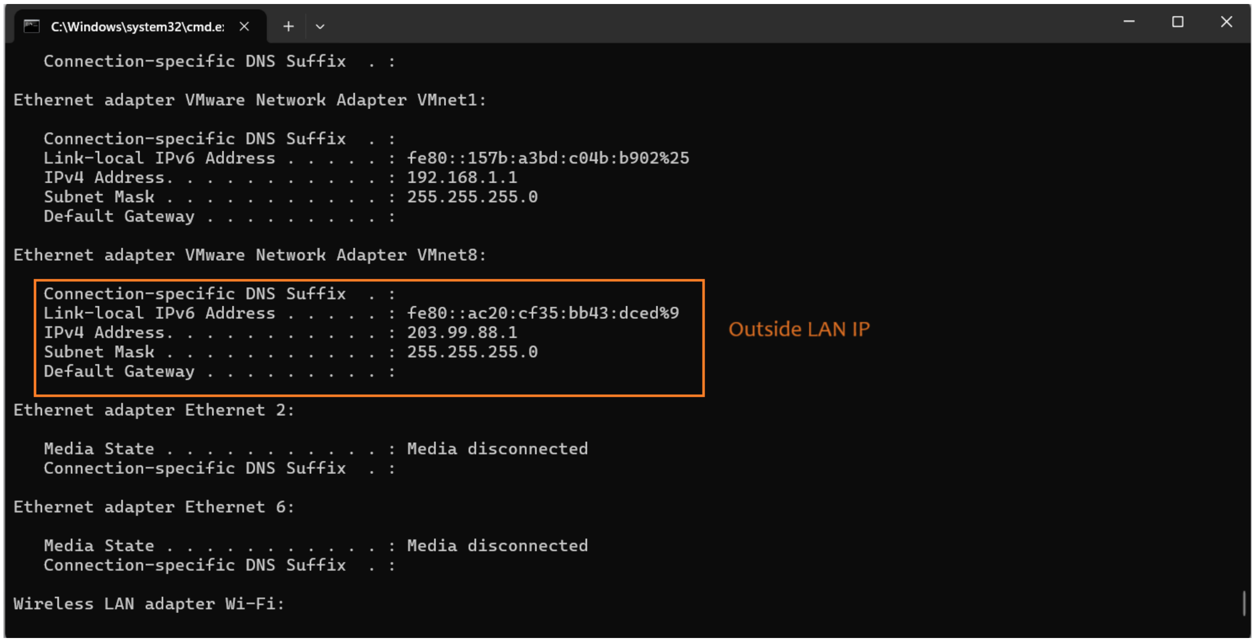
Check Logging From “ LAN-172.16.0.10” To “8.8.8.8”



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		✓ 260 B / 400 B	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		✓	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)

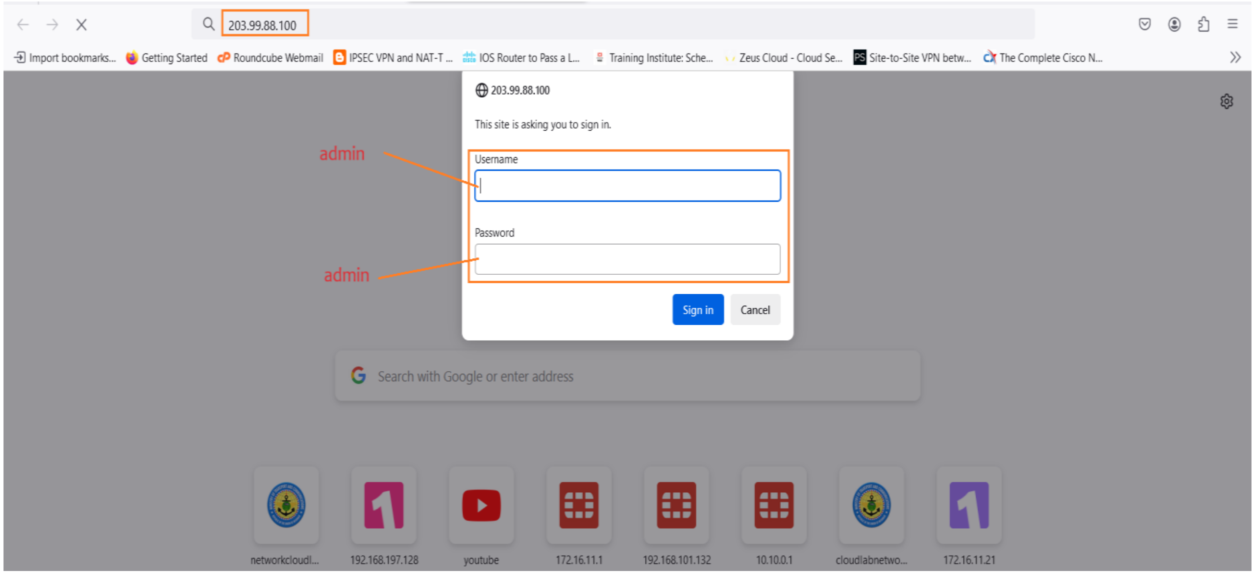
Check Public Web Server Access From “Public”

Check Lan IP



```
   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)



203.99.88.100

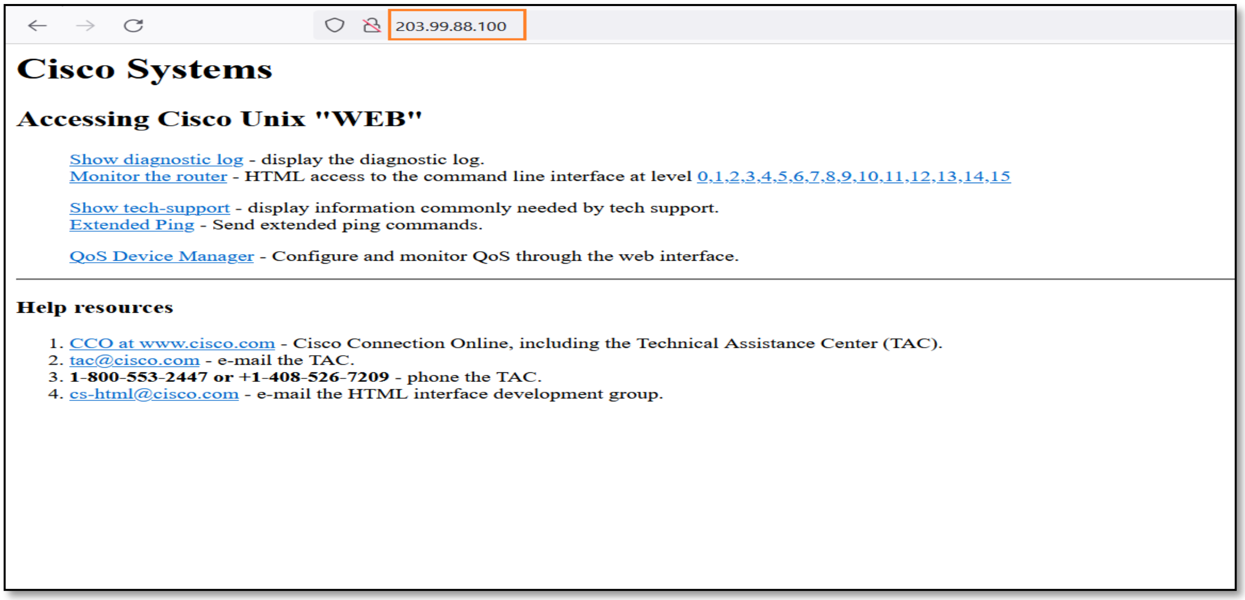
203.99.88.100

This site is asking you to sign in.

Username — admin

Password — admin

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



203.99.88.100

Cisco Systems

Accessing Cisco Unix "WEB"

Show diagnostic log - display the diagnostic log.
Monitor the router - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

Show tech-support - display information commonly needed by tech support.
Extended Ping - Send extended ping commands.

QoS Device Manager - Configure and monitor QoS through the web interface.

Help resources

1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. **1-800-553-2447 or +1-408-526-7209** - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.

Aung Zin Phyo

Sr.Network Engineer

+95-9897842856