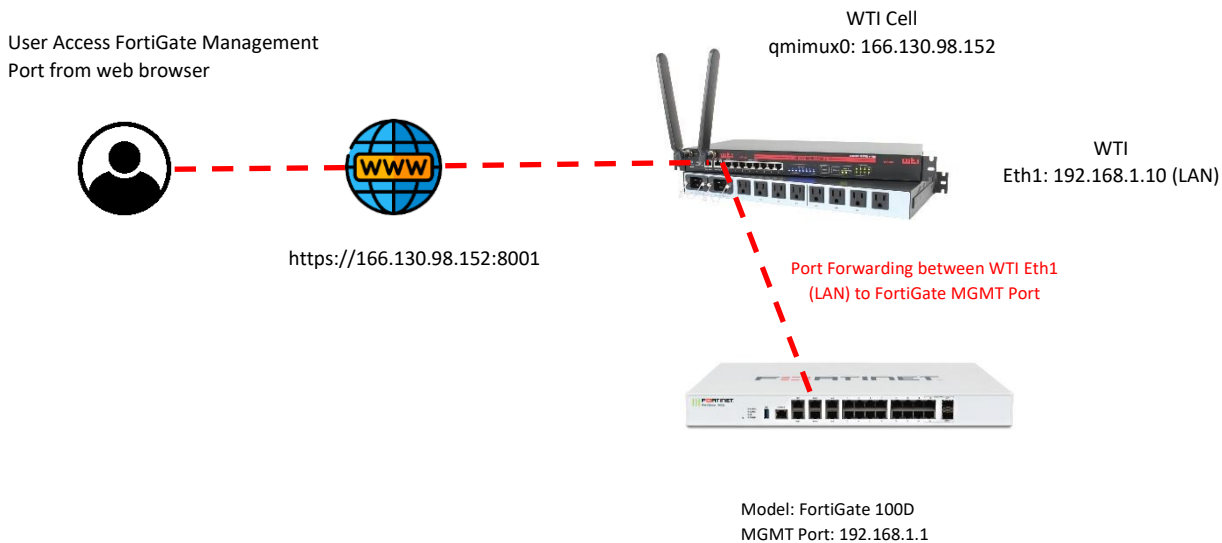


Cell - Port Forwarding to FortiGate Management Port



From WTI Device

Cell (qmimux0): 166.130.98.152
Eth1: 192.168.1.10 (LAN)

From Palo Alto Firewall

MGMT Port: 192.168.1.1
Static Route Default GW: 192.168.1.10

Configure IPTABLES from WTI device

From CLI enter /n option 5 and add the following IPTABLES as below.

Allow traffic from the LAN side

1. **iptables -A INPUT -i eth1 -j ACCEPT**

Allow established connections

2. **iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT**

Masquerade.

3. **iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE**

forwarding

4. **iptables -A FORWARD -i eth1 -o qmimux0 -m state --state RELATED,ESTABLISHED -j ACCEPT**

Allow outgoing connections from the LAN side.

5. **iptables -A FORWARD -i qmimux0 -o eth1 -j ACCEPT**

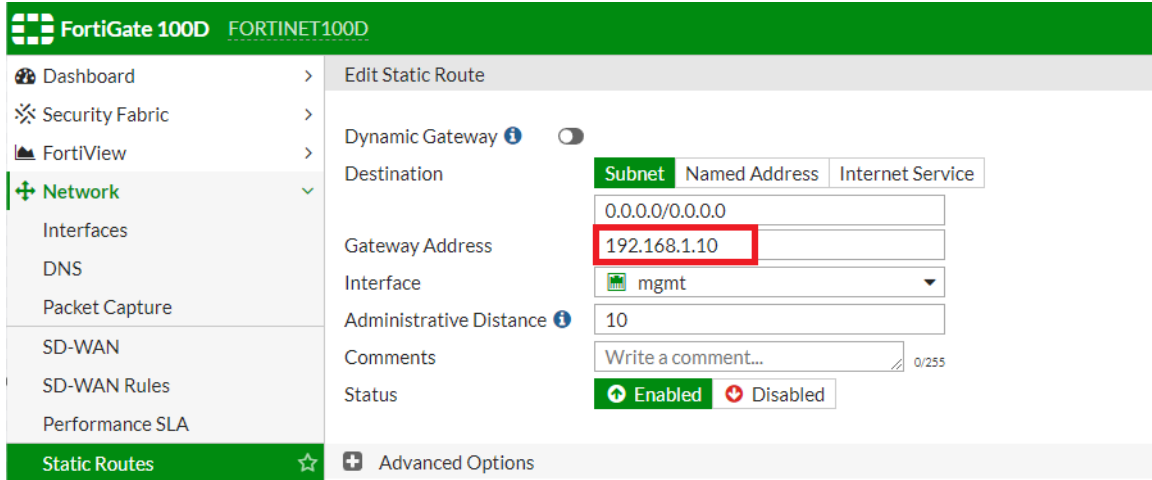
6. **iptables -t nat -A PREROUTING -p tcp -i qmimux0 --dport 8001 -j DNAT --to-destination 192.168.1.1:443**

7. **iptables -A FORWARD -p tcp -d 192.168.1.1 --dport 443 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT**

From FortiGate Firewall

Add Static Route to MGMT interface

From FortiGate go to Network >> Static Routes >> Create New and add the following to match the Gateway Address of WTI Eth0 (LAN).



FortiGate 100D FORTINET100D

Dashboard > Edit Static Route

Security Fabric >

FortiView >

Network >

Interfaces

DNS

Packet Capture

SD-WAN

SD-WAN Rules

Performance SLA


Static Routes ☆ + Advanced Options

Dynamic Gateway

Destination **Subnet** Named Address Internet Service

0.0.0.0/0.0.0.0

Gateway Address **192.168.1.10**

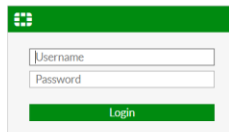
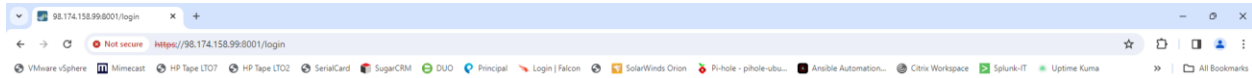
Interface  mgmt

Administrative Distance **10**

Comments Write a comment... 0/255

Status Enabled Disabled

Now go to web browser as <https://166.130.98.152:8001> and enter username/password of FortiGate Firewall.



FortiGate

Username

Password

Login