Abdelrahman Mohamed Ali Mahmoud

Group: CAI1_ISS8_S1e Fortinet Cybersecurity Engineer

Graduation project

SD-WAN Implementation

Objectives

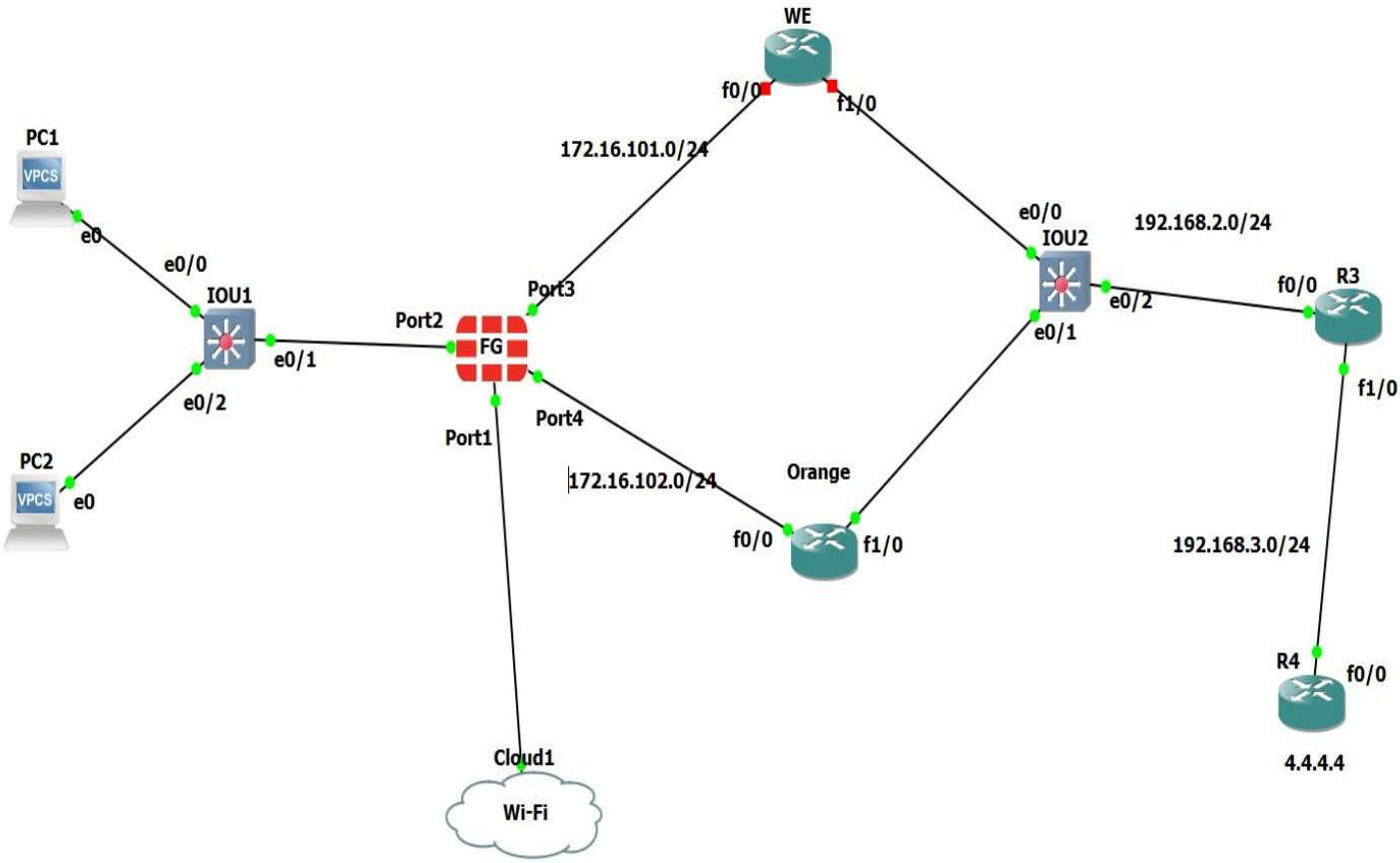
- Configure SD-WAN members and an SD-WAN zo
- Configure routes
- Configure SD-WAN rules for an internet servic
- Configure firewall policies
- Verify SD-WAN traffic distribution and event

Used Devices

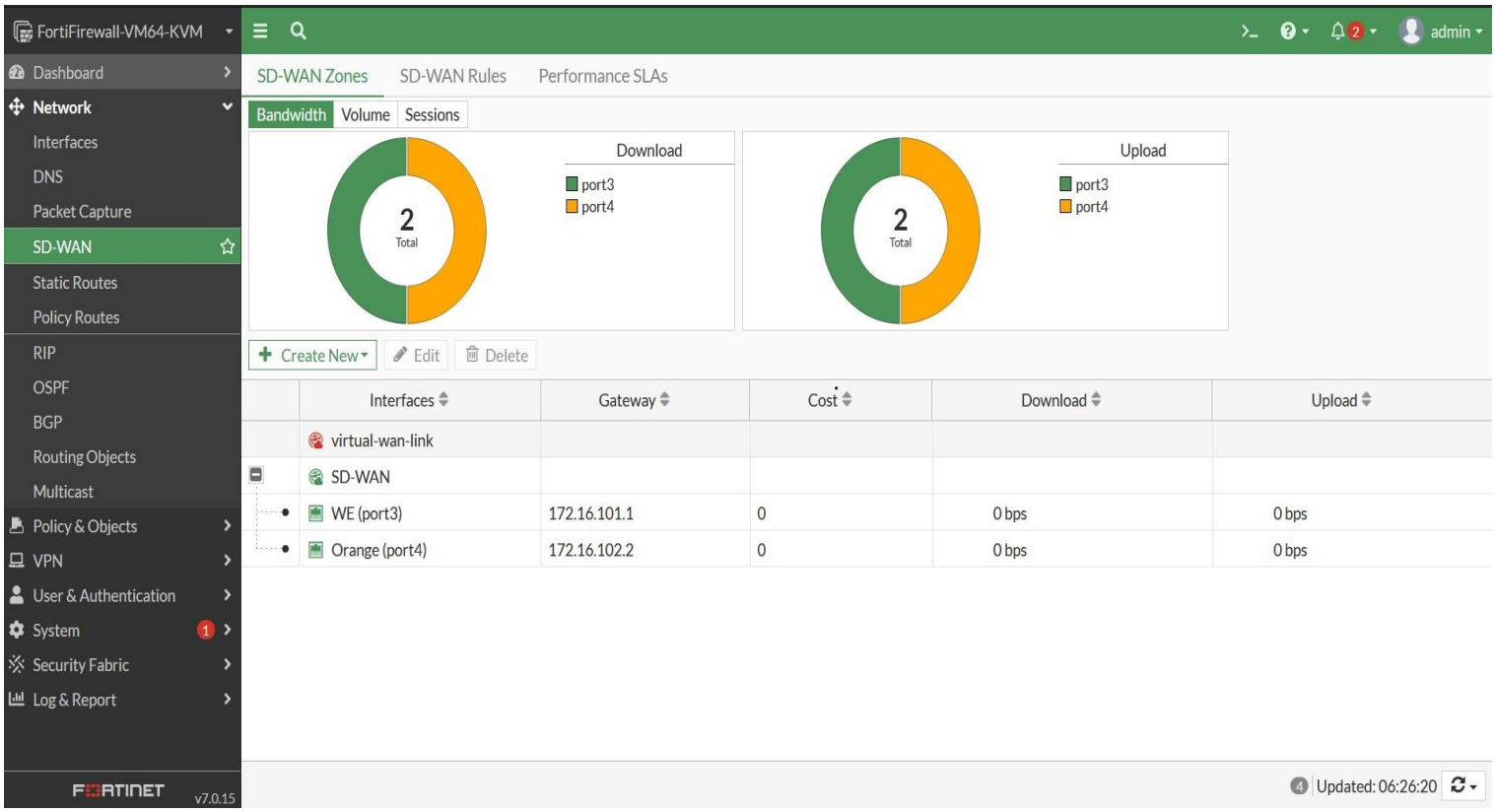
- 4- cisco routers
- 2- cisco switches
- 1- FortiGate firewall
- 2 virtual PCs

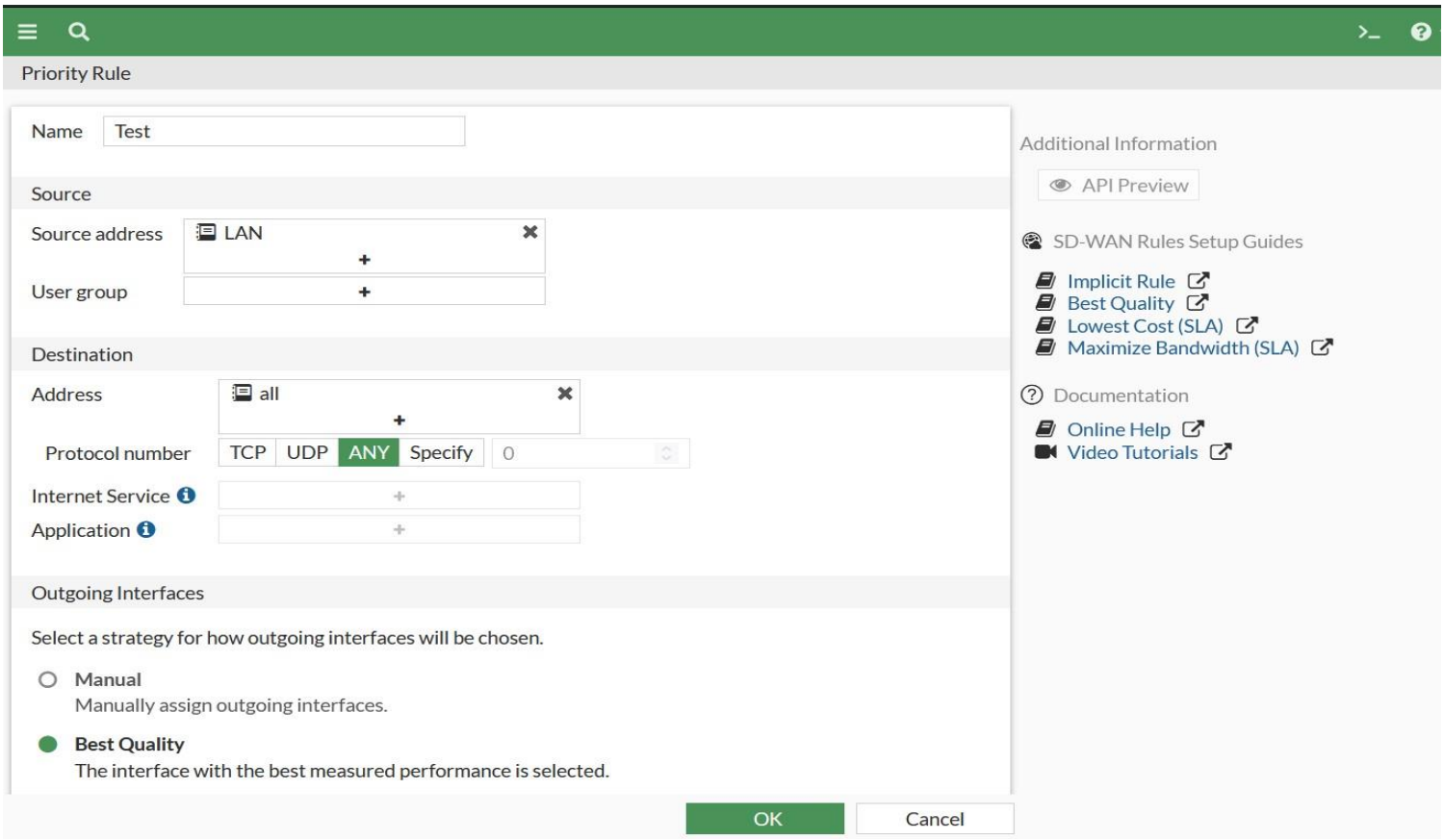
Implementation of SD-WAN configuration and test.

This part includes the topology of the network and the used devices to test the SD-WAN and verify it’s working.

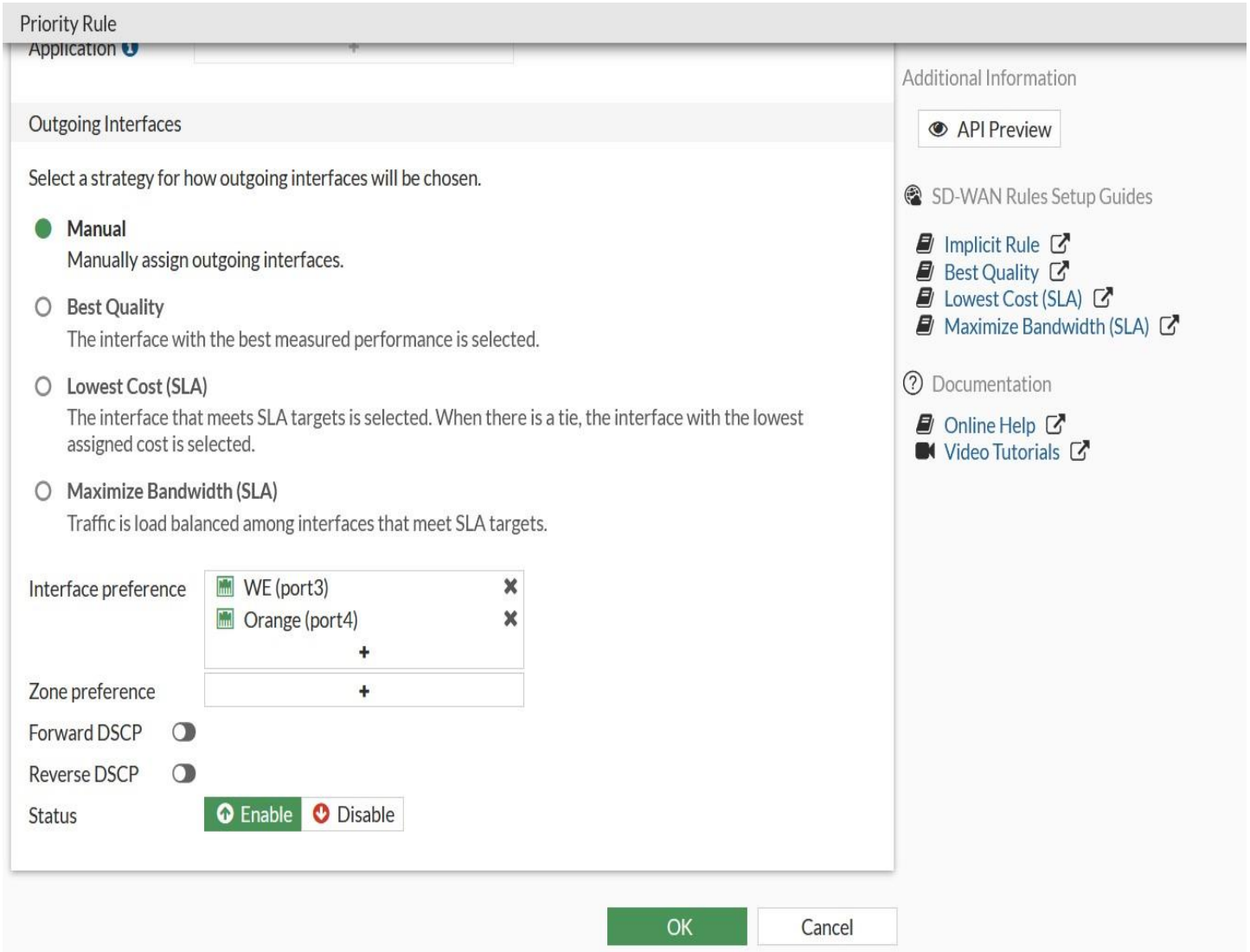


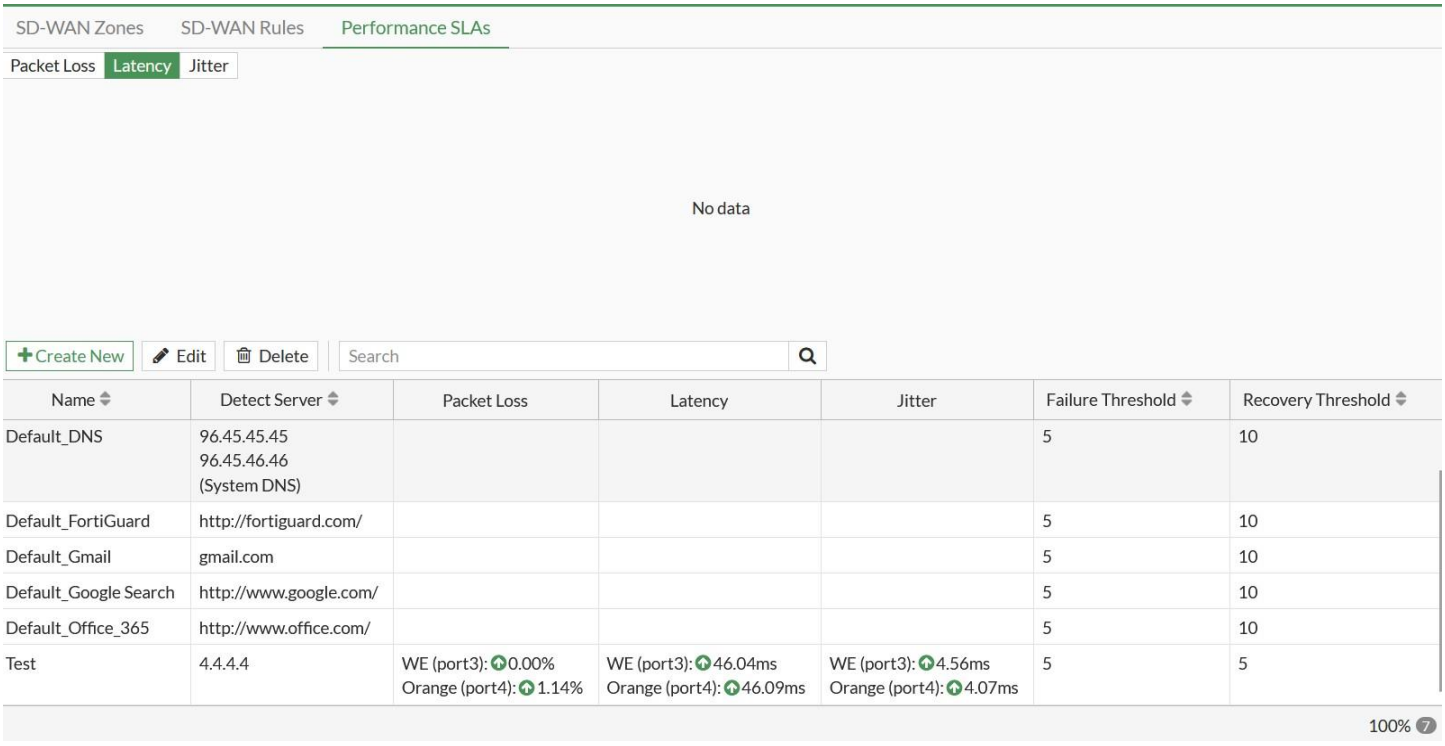
This picture show the SD-WAN zone created and it’s two members of the ISP (We, Orange)





Configuring the priority role for the SD-WAN zone

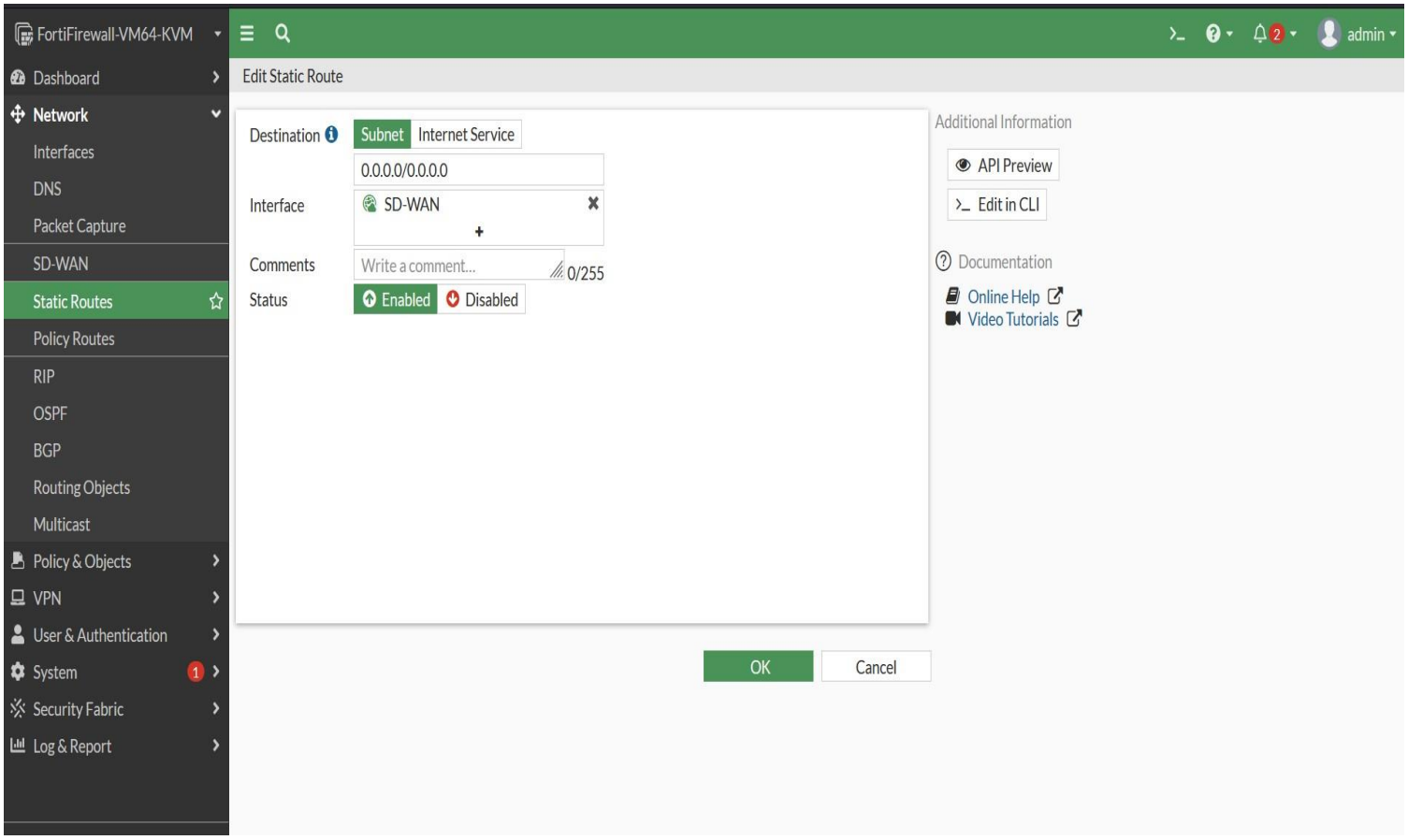




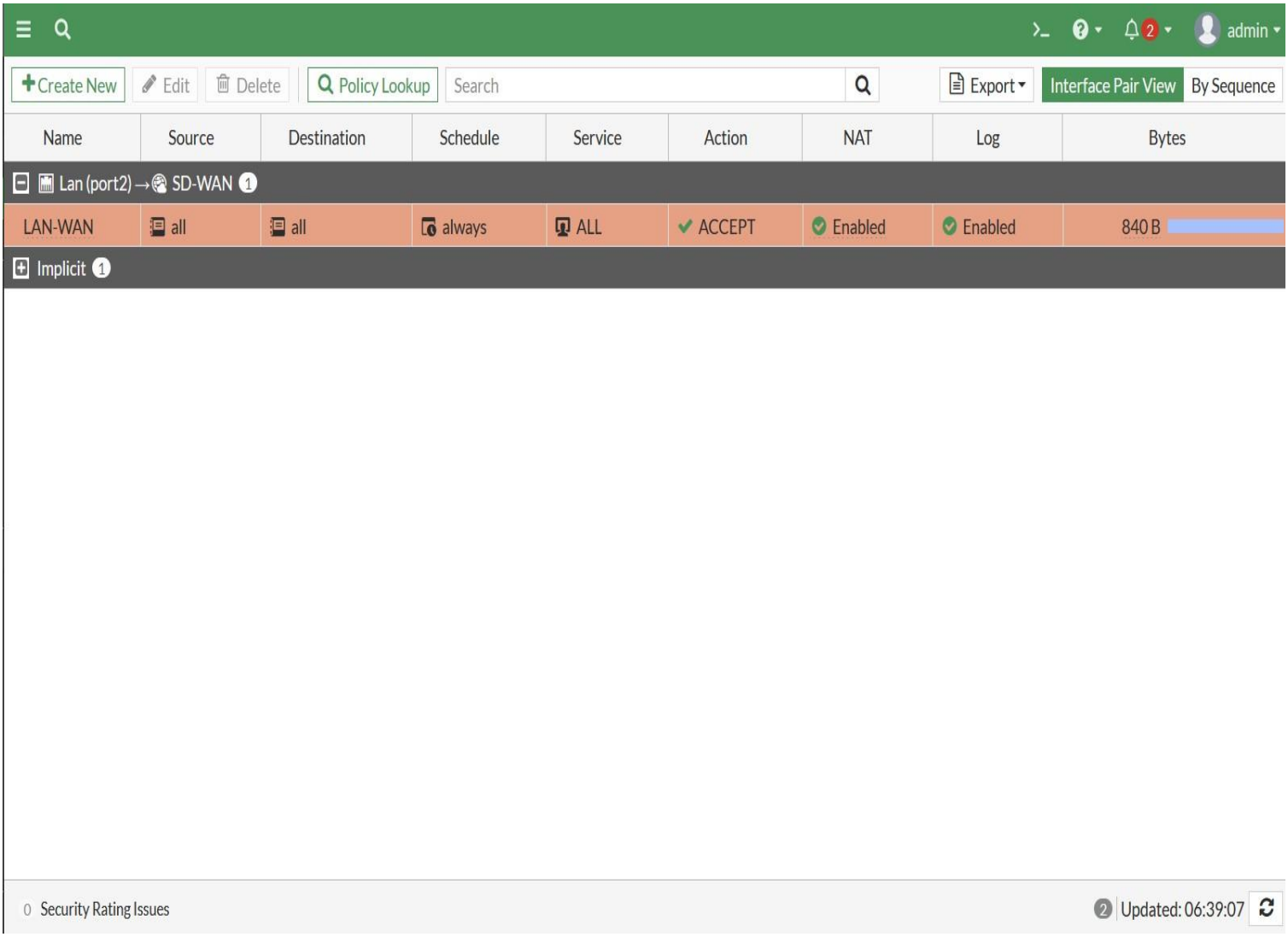
Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
Default_DNS	96.45.45.45 96.45.46.46 (System DNS)				5	10
Default_FortiGuard	http://fortiguard.com/				5	10
Default_Gmail	gmail.com				5	10
Default_Google Search	http://www.google.com/				5	10
Default_Office_365	http://www.office.com/				5	10
Test	4.4.4.4	WE (port3): 0.00% Orange (port4): 1.14%	WE (port3): 46.04ms Orange (port4): 46.09ms	WE (port3): 4.56ms Orange (port4): 4.07ms	5	5

100%

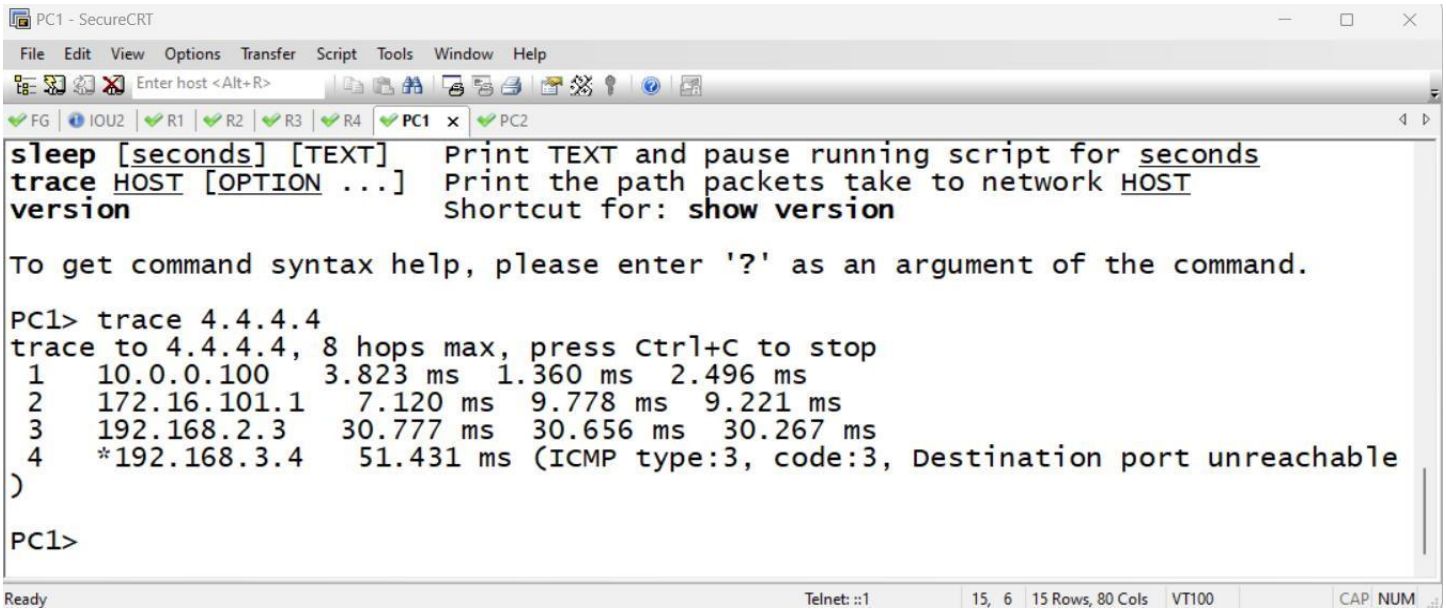
Create a static route


FortiFirewall-VM64-KVM
admin
Dashboard
Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
VPN
User & Authentication
System
Security Fabric
Log & Report
Edit Static Route
Destination
Subnet
Internet Service
0.0.0.0/0.0.0.0
Interface
SD-WAN
Comments
Write a comment...
0/255
Status
Enabled
Disabled
Additional Information
API Preview
Edit in CLI
Documentation
Online Help
Video Tutorials
OK
Cancel

Create a policy to allow the traffic from Lan to Wan (port2 ==➔ port1)



Test ISP1 We



Test ISP2 Orange