Week 3

SD-WAN Implementation Documentation

Introduction & Purpose of SD-WAN

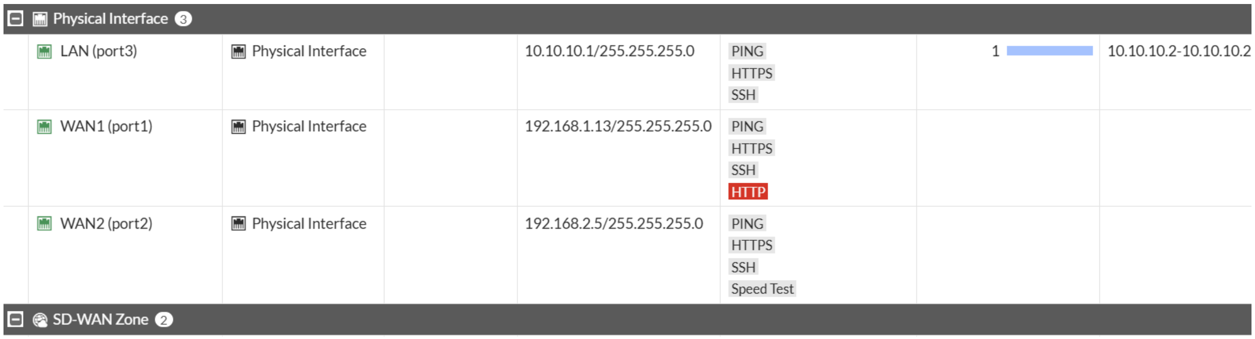
SD-WAN (Software-Defined Wide Area Network) is an advanced solution for managing WAN networks that provides:

- The ability to combine multiple internet connections (WAN links) for smart traffic distribution.
- Quality-based routing to optimize traffic depending on the service type (e.g., VoIP, Video, Web).
- **Automatic failover** if one link goes down, ensuring uninterrupted user experience.
- **Load balancing** to utilize all available links efficiently.
- Continuous performance monitoring (latency, jitter, packet loss) to improve network reliability.

In short: SD-WAN makes the network more intelligent, flexible, and reliable compared to a single fixed WAN link.

Project Environment

- **Number of Internet Links:** 2 WAN links
- **Local Network:** 10.10.10.0/24
- **Device:** FortiGate Firewall
- **Goal:** Route internal traffic to the internet efficiently and manage traffic based on service type (e.g., VoIP calls, YouTube streaming).

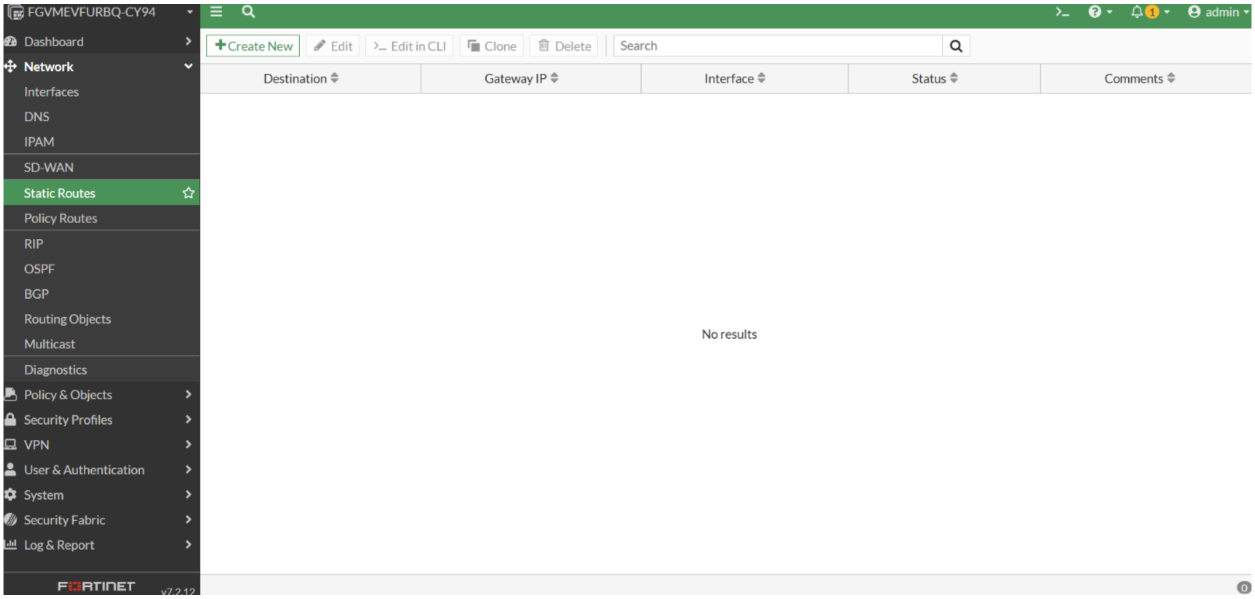


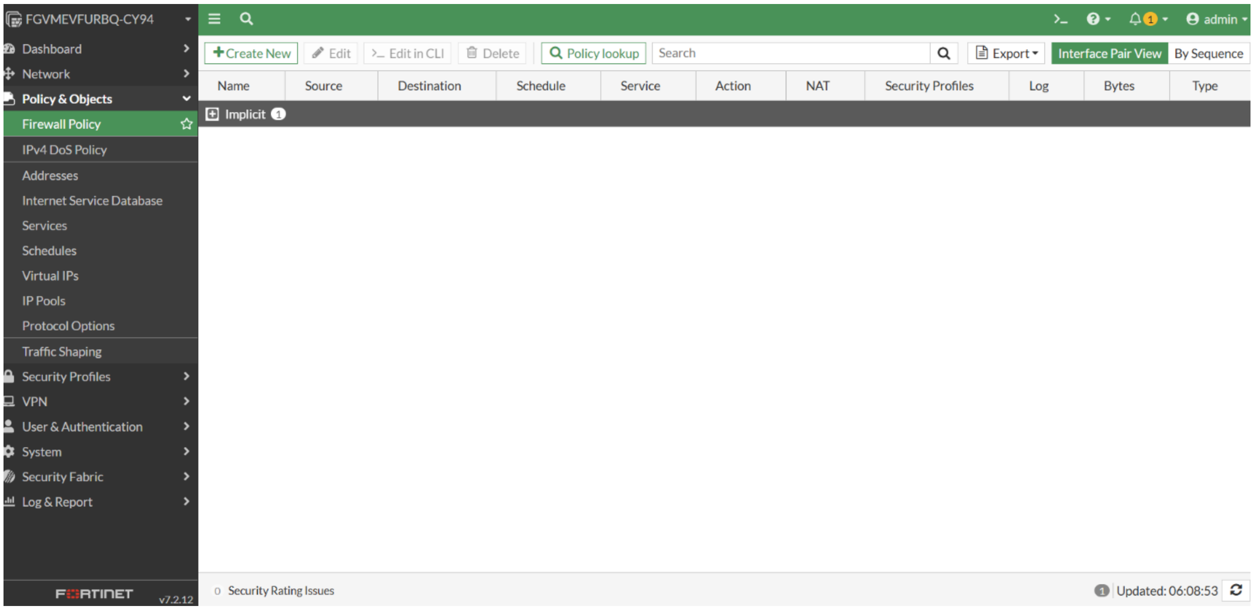
⊟ Physical Interface 3						
LAN (port3)	Physical Interface		10.10.10.1/255.255.255.0	PING HTTPS SSH	1	10.10.10.2-10.10.10.2
WAN1 (port1)	Physical Interface		192.168.1.13/255.255.255.0	PING HTTPS SSH HTTP		
WAN2 (port2)	Physical Interface		192.168.2.5/255.255.255.0	PING HTTPS SSH Speed Test		
⊟ SD-WAN Zone 2						

Implementation Steps

Step 1: Verify Initial Configuration

- Checked Firewall Policies: No policies are active.
- Checked Routing: No static routes or default routes exist.
- **Purpose:** Ensure a clean environment before enabling SD-WAN.



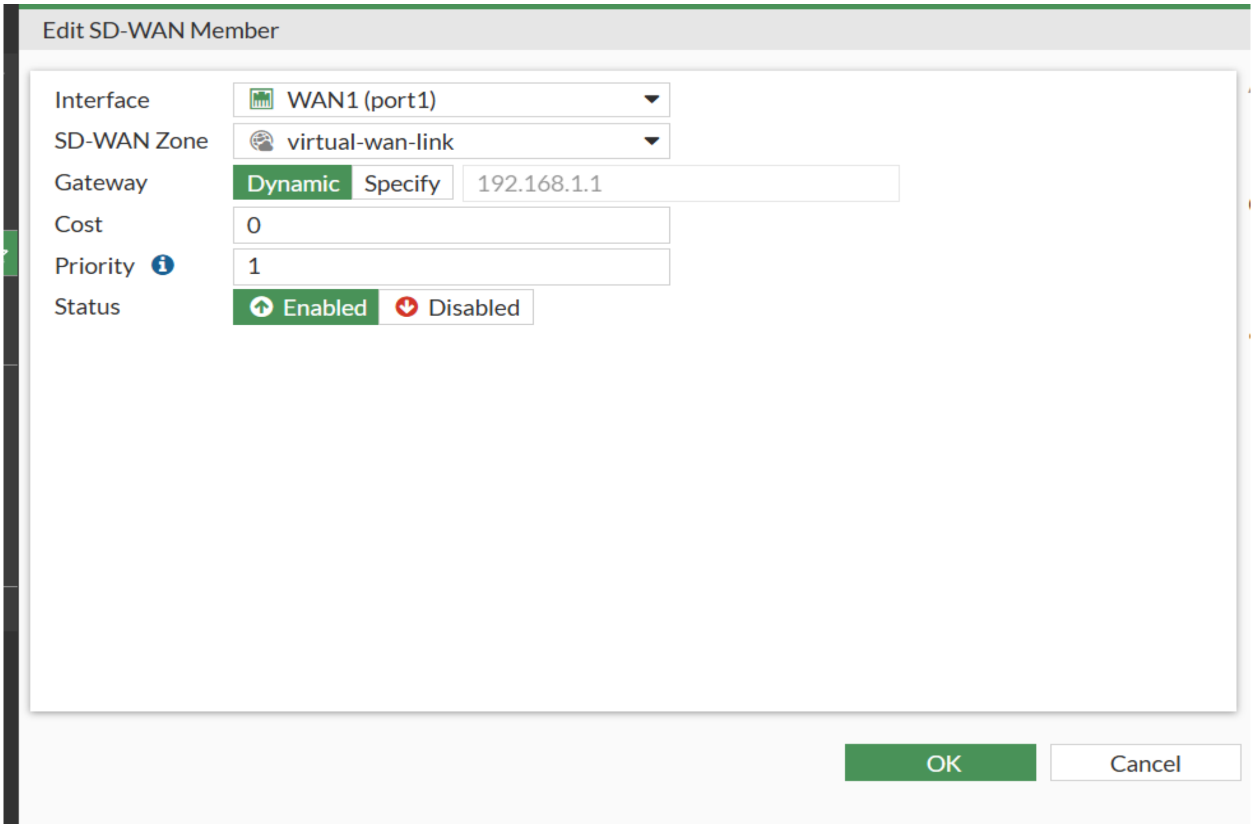


Step 2: Add Internet Links as SD-WAN Members

- Each WAN link is added as a **Member** inside SD-WAN:
  - WAN1 → Member 1

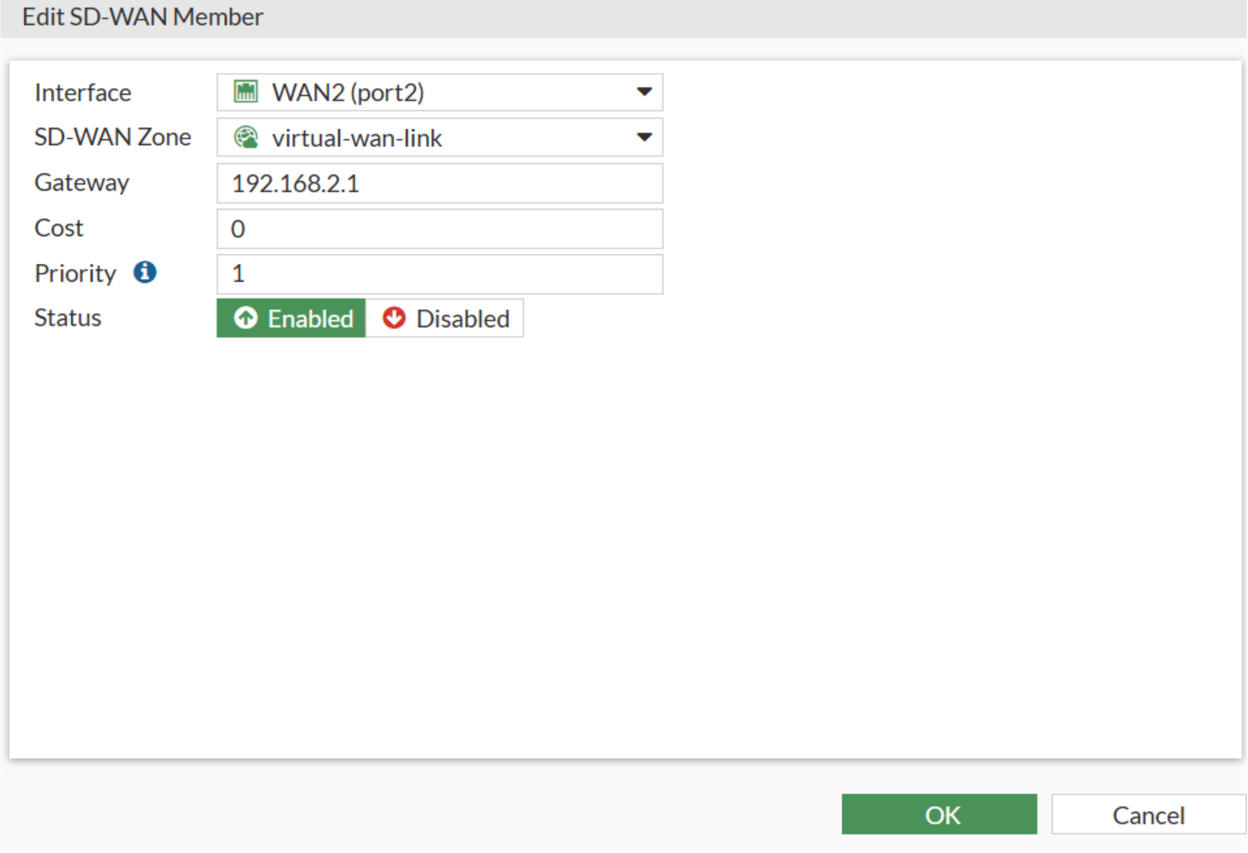
    - WAN2 → Member 2

- **Purpose:** Integrate all WAN links under a single SD-WAN zone for centralized management.



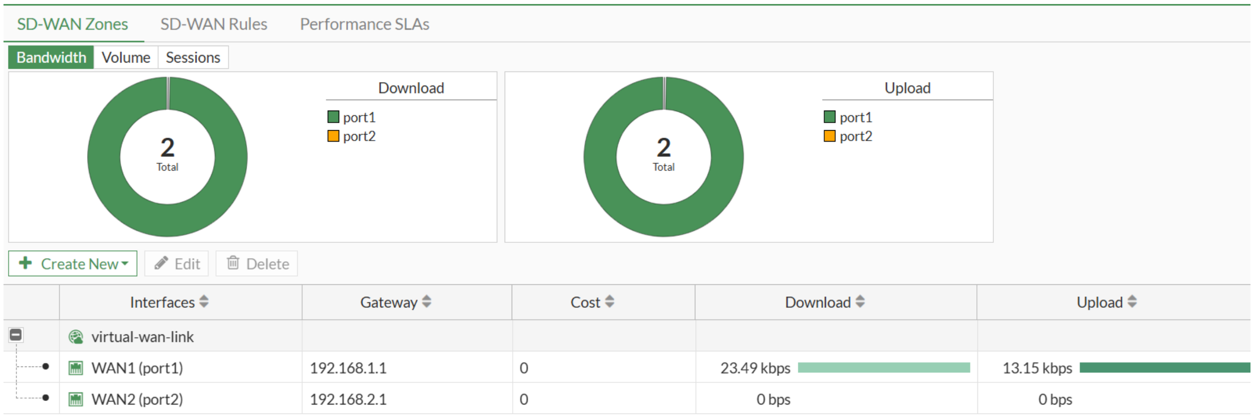
Edit SD-WAN Member

Interface	WAN1 (port1)
SD-WAN Zone	virtual-wan-link
Gateway	[✓ Dynamic] Specify 192.168.1.1
Cost	0
Priority	1
Status	[✓ Enabled] Disabled



Edit SD-WAN Member

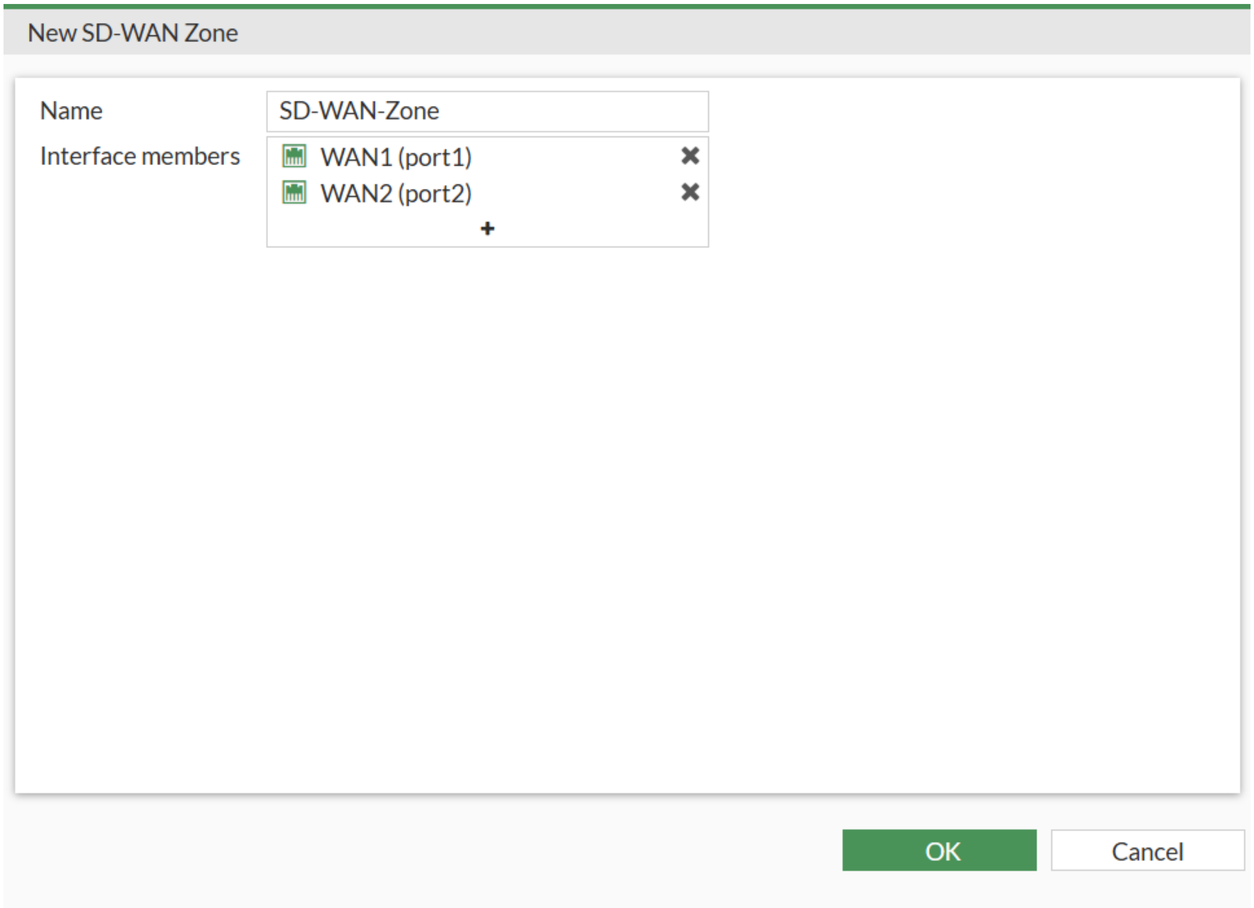
Interface	WAN2 (port2)
SD-WAN Zone	virtual-wan-link
Gateway	192.168.2.1
Cost	0
Priority	1
Status	Enabled ● Disabled



Interfaces	Gateway	Cost	Download	Upload
virtual-wan-link				
WAN1 (port1)	192.168.1.1	0	23.49 kbps	13.15 kbps
WAN2 (port2)	192.168.2.1	0	0 bps	0 bps

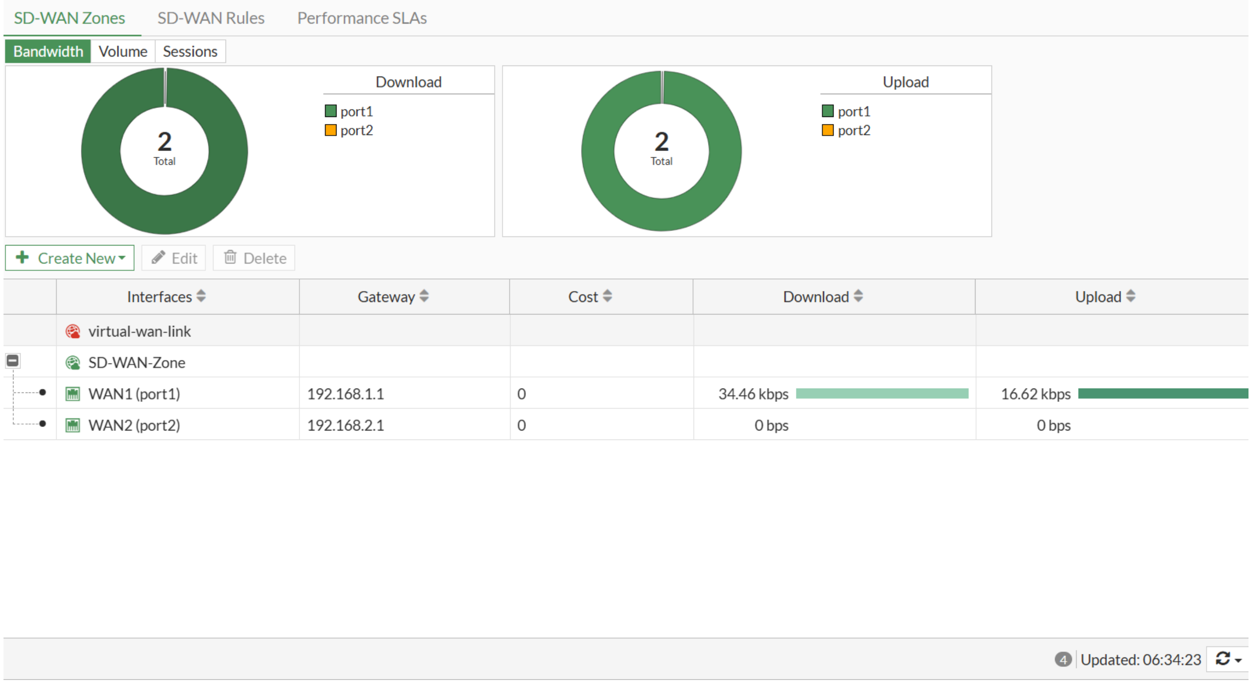
Step 3: Create SD-WAN Zone

- Created a **SD-WAN Zone** named SD-WAN-Zone.
- Added all WAN members (WAN1, WAN2) into this zone.



New SD-WAN Zone

Name	SD-WAN-Zone
Interface members	WAN1 (port1) WAN2 (port2)

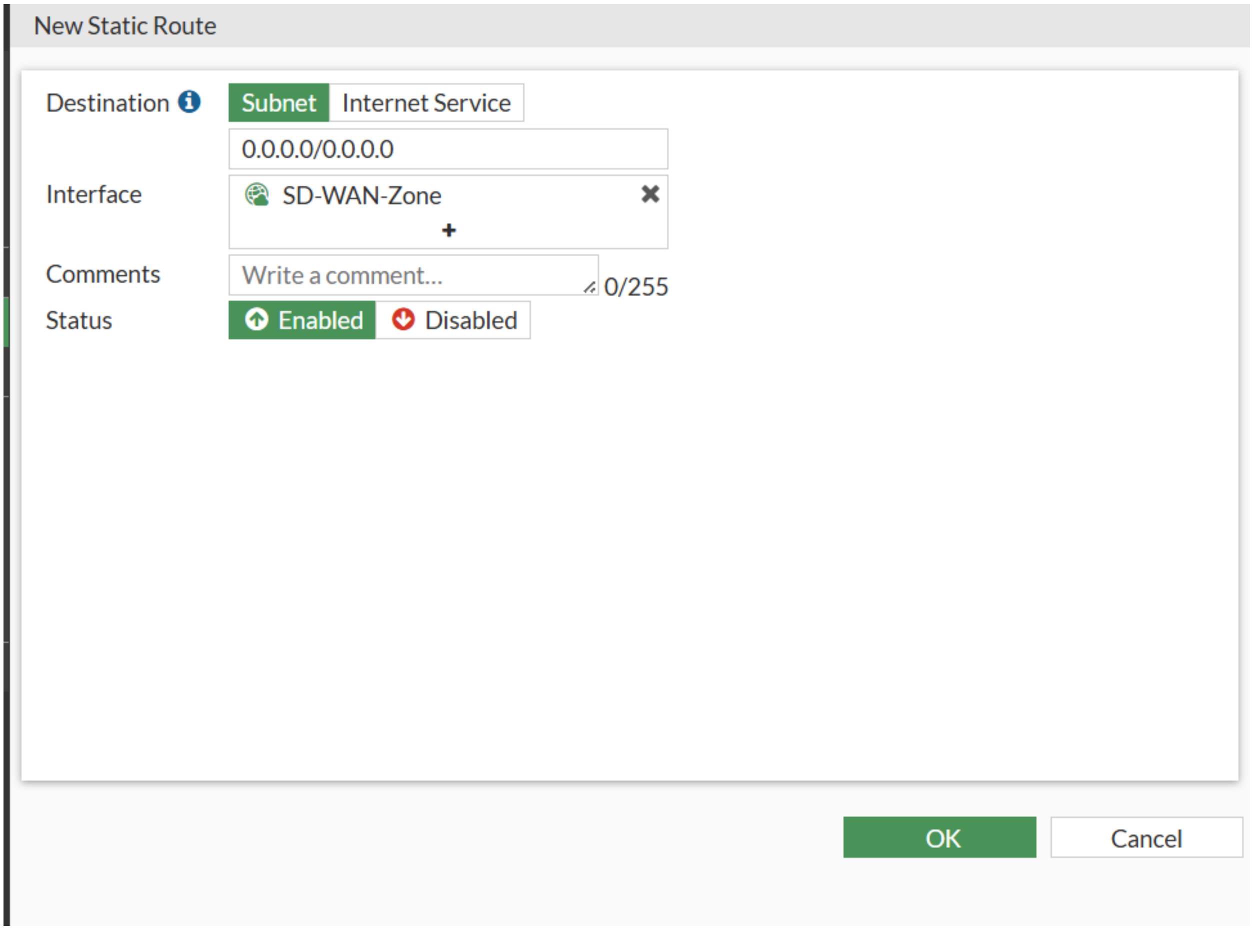


Interfaces	Gateway	Cost	Download	Upload
virtual-wan-link				
SD-WAN-Zone				
WAN1 (port1)	192.168.1.1	0	34.46 kbps	16.62 kbps
WAN2 (port2)	192.168.2.1	0	0 bps	0 bps

Updated: 06:34:23

Step 4: Configure Default Static Route

- **Static Route Configuration:**
  - **Destination:** 0.0.0.0/0
  - **Interface:** SD-WAN-Zone
- **Purpose:** Direct all outbound traffic through the SD-WAN zone instead of individual WAN interfaces.



New Static Route

Destination: Subnet | Internet Service

0.0.0.0/0.0.0.0

Interface: SD-WAN-Zone

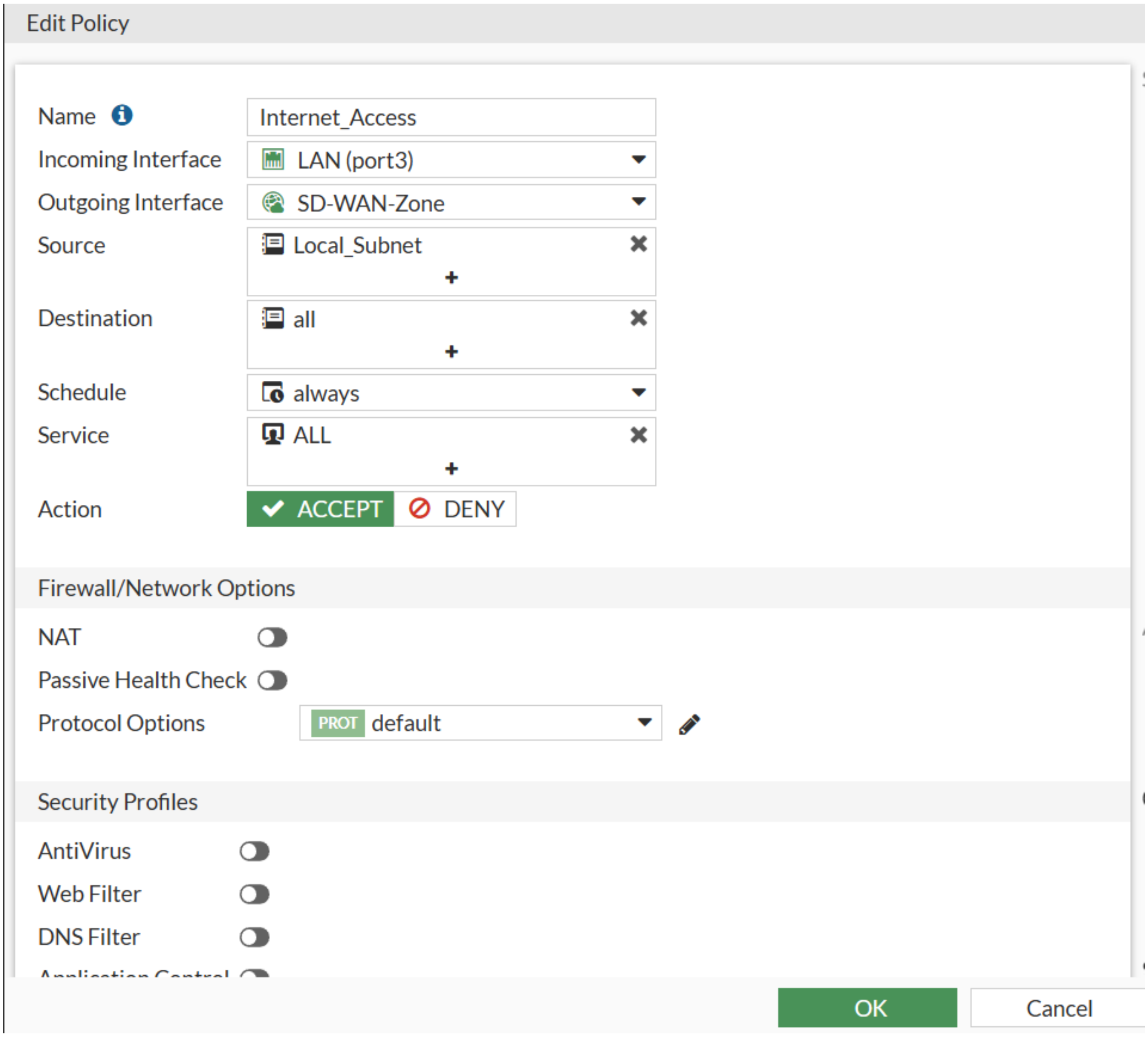
Comments: Write a comment... 0/255

Status: Enabled | Disabled

Step 5: Configure Firewall Policy

- Created a firewall policy named Internet Access:
  - **Incoming Interface:** LAN
  - **Outgoing Interface:** SD-WAN-Zone

  - **Source:** Local Subnet 10.10.10.0/24
  - **Destination:** All
  - **Schedule:** All
  - **Service:** All
- **Purpose:** Ensure internal traffic exits to the internet via the SD-WAN zone.



Edit Policy

Name: Internet_Access

Incoming Interface: LAN (port3)

Outgoing Interface: SD-WAN-Zone

Source: Local_Subnet

Destination: all

Schedule: always

Service: ALL

Action: [✓ ACCEPT] DENY

Firewall/Network Options

NAT: ○

Passive Health Check: ○

Protocol Options: PROT default

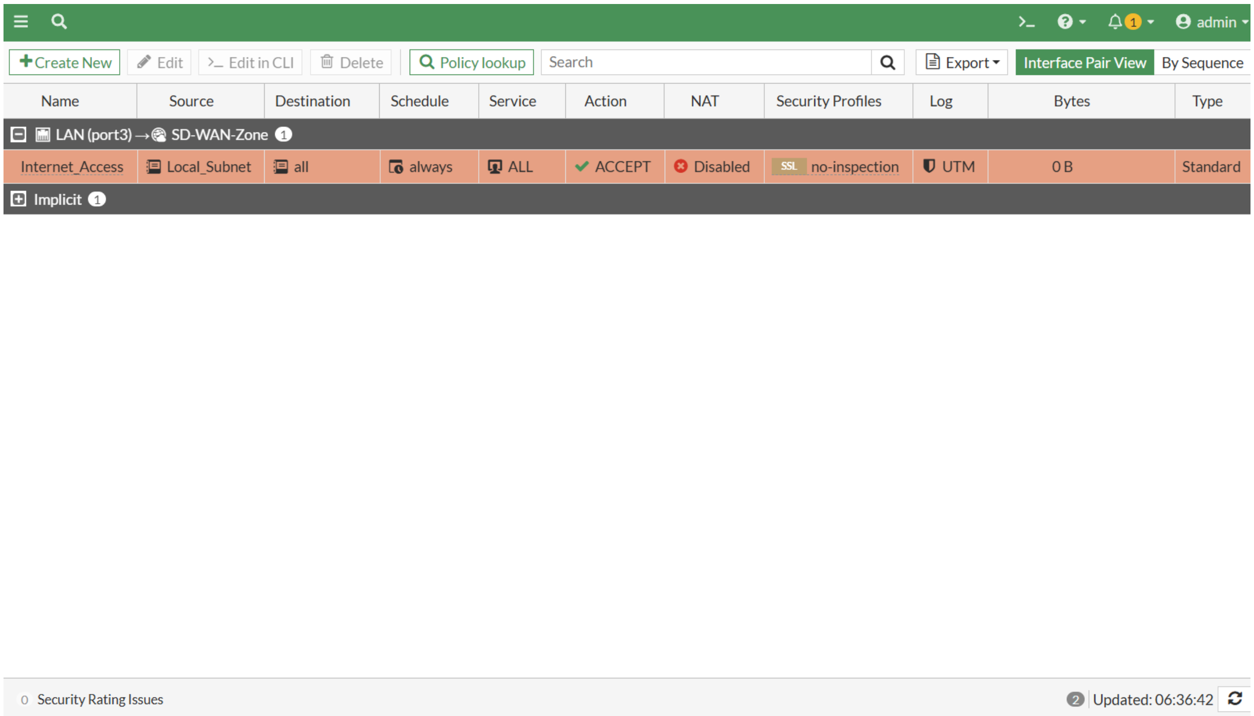
Security Profiles

AntiVirus: ○

Web Filter: ○

DNS Filter: ○

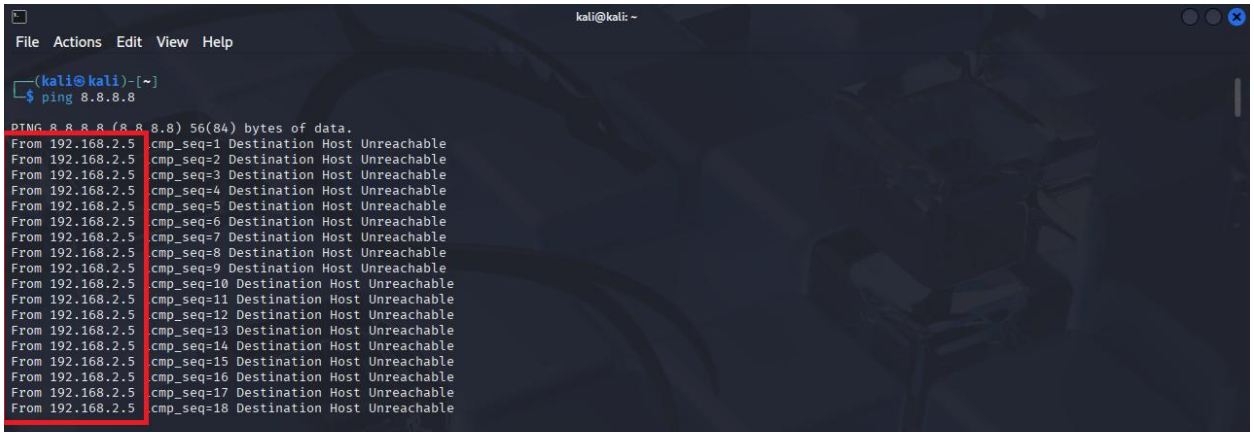
Application Control: ○



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type
LAN (port3) → SD-WAN-Zone 1										
Internet_Access	Local_Subnet	all	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	UTM	0 B	Standard
Implicit 1										

0 Security Rating Issues

2 Updated: 06:36:42

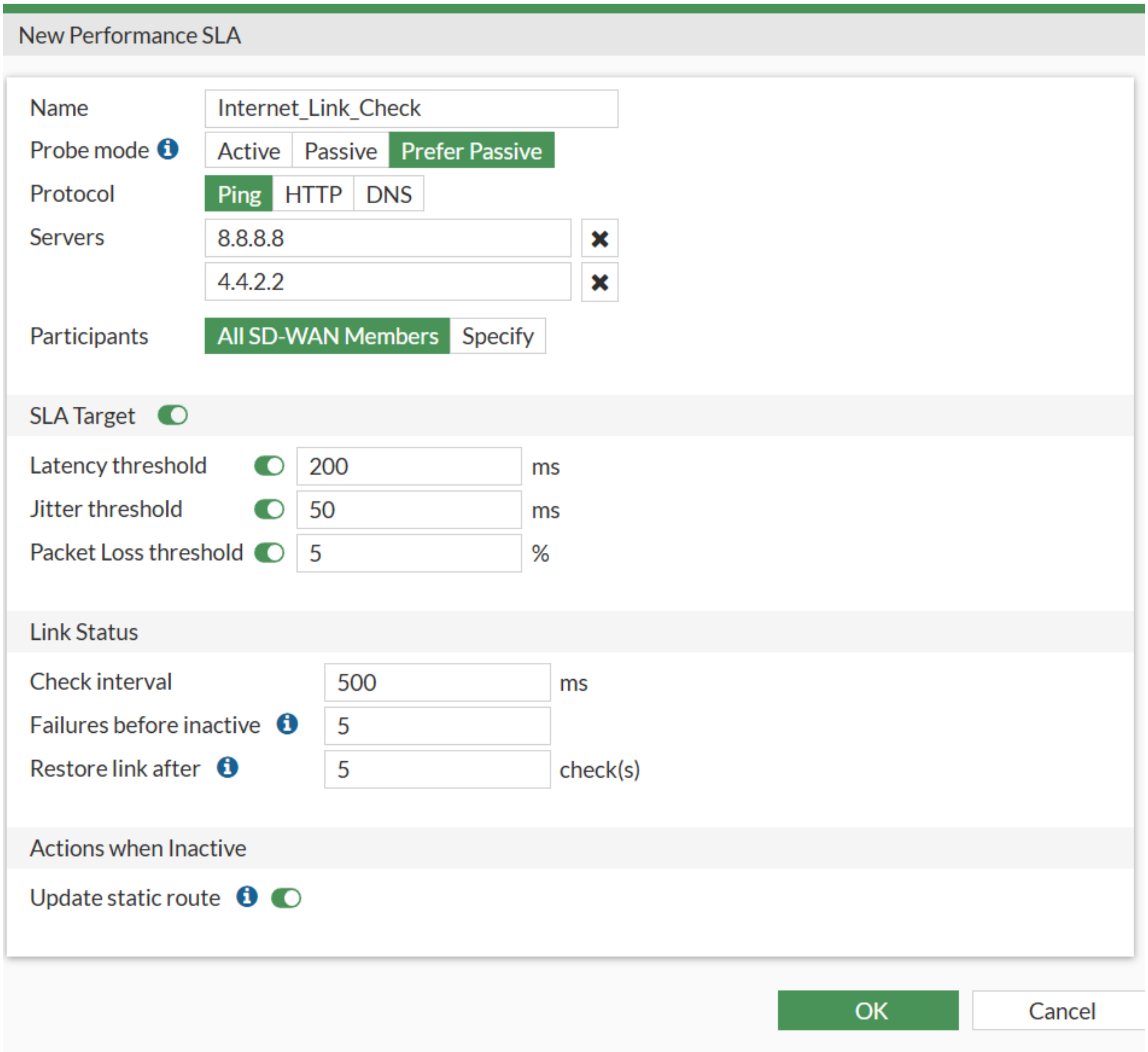


```
┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 192.168.2.5 icmp_seq=1 Destination Host Unreachable
From 192.168.2.5 icmp_seq=2 Destination Host Unreachable
From 192.168.2.5 icmp_seq=3 Destination Host Unreachable
From 192.168.2.5 icmp_seq=4 Destination Host Unreachable
From 192.168.2.5 icmp_seq=5 Destination Host Unreachable
From 192.168.2.5 icmp_seq=6 Destination Host Unreachable
From 192.168.2.5 icmp_seq=7 Destination Host Unreachable
From 192.168.2.5 icmp_seq=8 Destination Host Unreachable
From 192.168.2.5 icmp_seq=9 Destination Host Unreachable
From 192.168.2.5 icmp_seq=10 Destination Host Unreachable
From 192.168.2.5 icmp_seq=11 Destination Host Unreachable
From 192.168.2.5 icmp_seq=12 Destination Host Unreachable
From 192.168.2.5 icmp_seq=13 Destination Host Unreachable
From 192.168.2.5 icmp_seq=14 Destination Host Unreachable
From 192.168.2.5 icmp_seq=15 Destination Host Unreachable
From 192.168.2.5 icmp_seq=16 Destination Host Unreachable
From 192.168.2.5 icmp_seq=17 Destination Host Unreachable
From 192.168.2.5 icmp_seq=18 Destination Host Unreachable
```

Step 6: Configure Performance SLA

- **Name:** Internet_Link_Check
- **Probe Mode:** Prefer Passive
- **Protocol:** Ping
- **Servers:** 8.8.8.8, 4.4.2.2
- **Participated Members:** All SD-WAN Members

- **SLA Targets:**
  - Latency: 200ms
  - Jitter: 50ms
  - Packet Loss: 5%
- **Purpose:** Monitor link quality and enable intelligent routing decisions based on performance.



New Performance SLA

Name: Internet_Link_Check

Probe mode: Active Passive [✓ Prefer Passive]

Protocol: [✓ Ping] HTTP DNS

Servers:
8.8.8.8
4.4.2.2

Participants: [✓ All SD-WAN Members] Specify

SLA Target ●

Latency threshold ● 200 ms

Jitter threshold ● 50 ms

Packet Loss threshold ● 5 %

Link Status

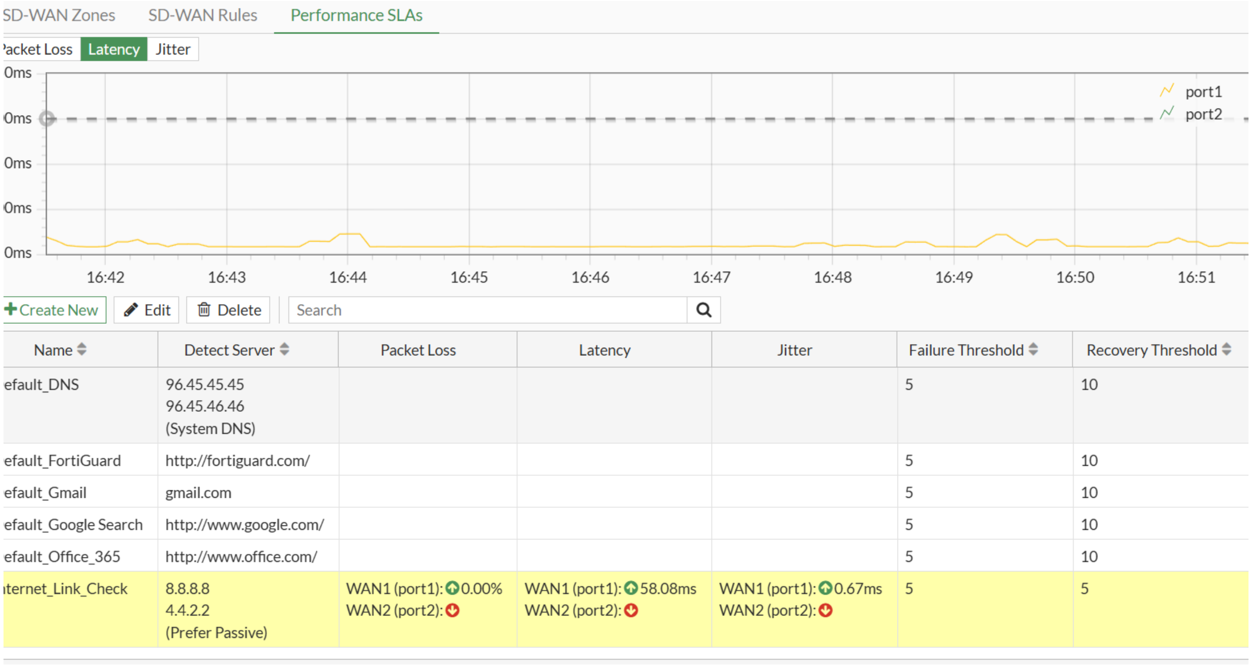
Check interval: 500 ms

Failures before inactive: 5

Restore link after: 5 check(s)

Actions when Inactive

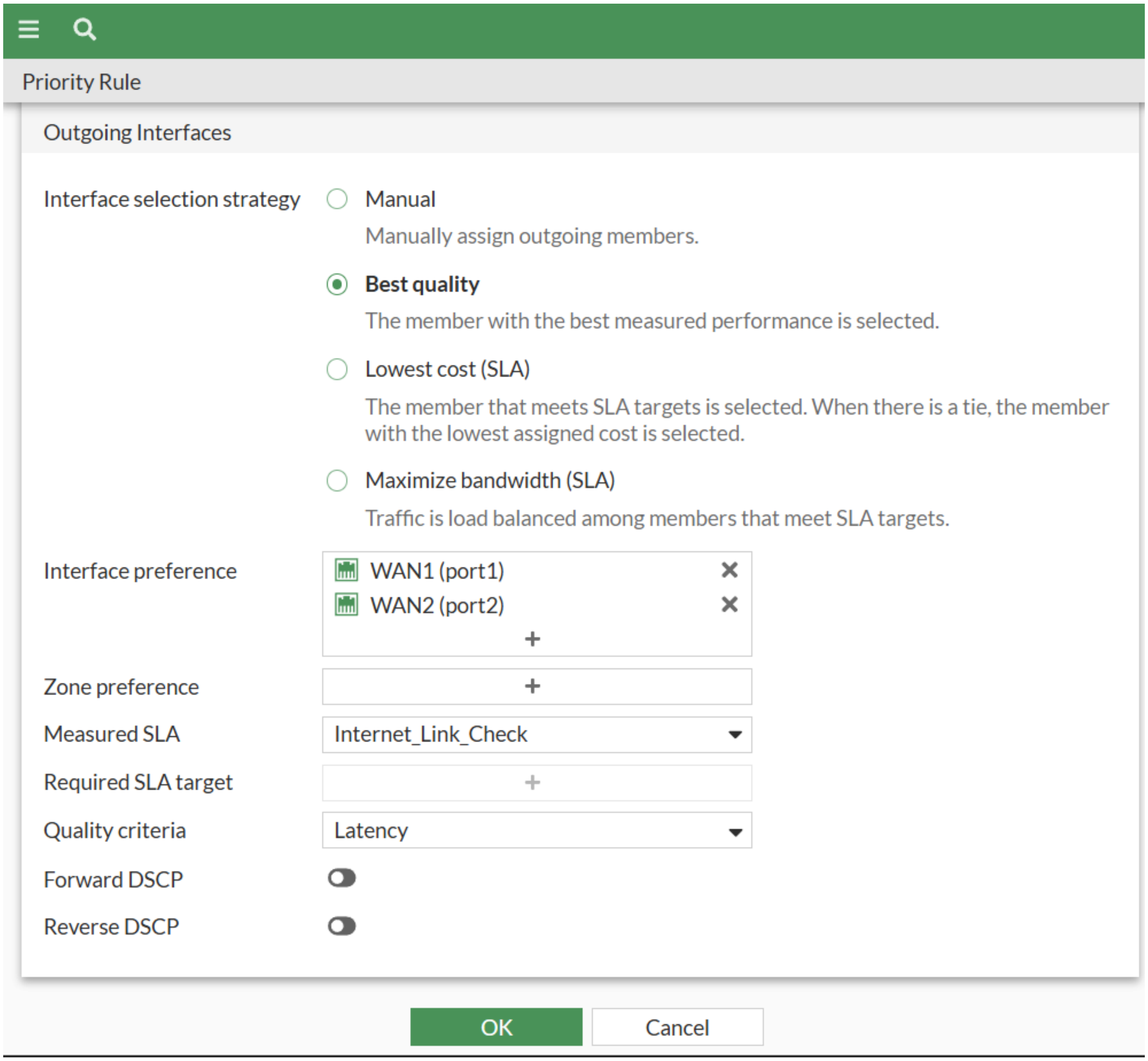
Update static route ●



Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
efault_DNS	96.45.45.45 96.45.46.46 (System DNS)				5	10
efault_FortiGuard	http://fortiguard.com/				5	10
efault_Gmail	gmail.com				5	10
efault_Google Search	http://www.google.com/				5	10
efault_Office_365	http://www.office.com/				5	10
iternet_Link_Check	8.8.8.8 4.4.2.2 (Prefer Passive)	WAN1 (port1): ⬆0.00% WAN2 (port2): ⬇	WAN1 (port1): ⬆58.08ms WAN2 (port2): ⬇	WAN1 (port1): ⬆0.67ms WAN2 (port2): ⬇	5	5

Step 7: Create SD-WAN Rules

- Example rules implemented:
  - Traffic from subnet 10.10.10.0/24 to **YouTube** → routed via **WAN1**
  - Traffic from subnet 10.10.10.0/24 for **VoIP calls** → routed via the **best performing link** automatically
- **Purpose:** Direct traffic efficiently based on application type and link quality.



Priority Rule

Outgoing Interfaces

Interface selection strategy
○ Manual
Manually assign outgoing members.
● **Best quality**
The member with the best measured performance is selected.
○ Lowest cost (SLA)
The member that meets SLA targets is selected. When there is a tie, the member with the lowest assigned cost is selected.
○ Maximize bandwidth (SLA)
Traffic is load balanced among members that meet SLA targets.

Interface preference: WAN1 (port1), WAN2 (port2)

Zone preference: +

Measured SLA: Internet_Link_Check

Required SLA target: +

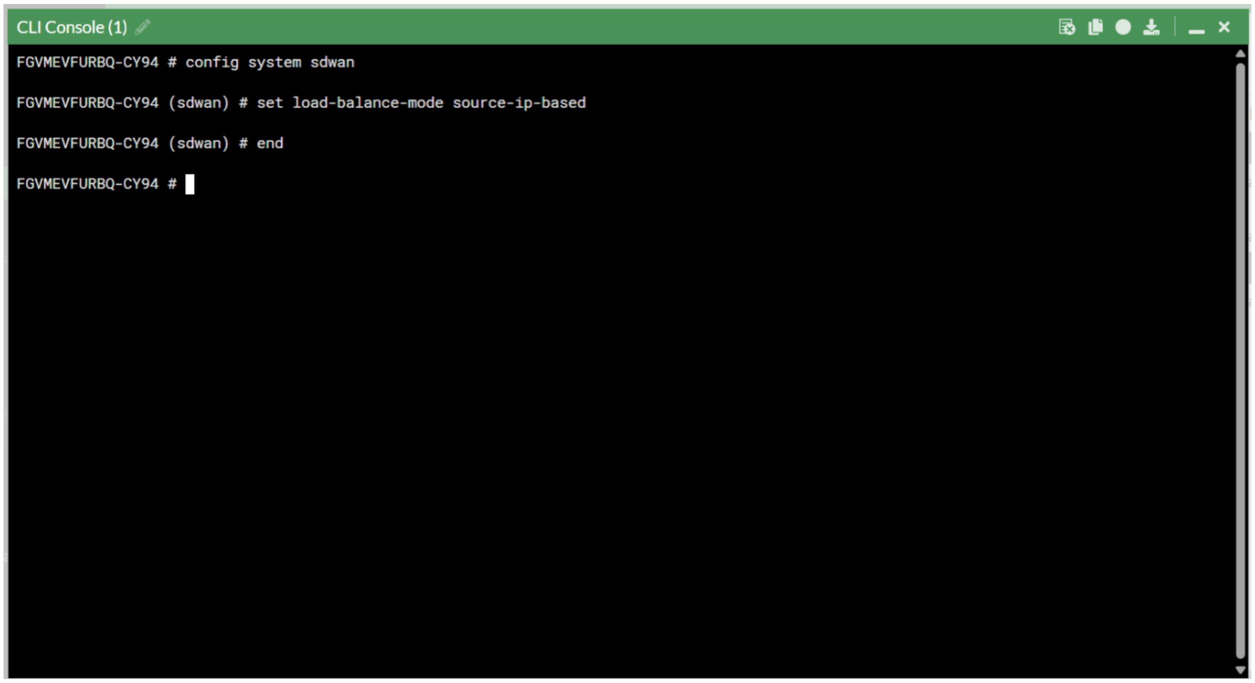
Quality criteria: Latency

Forward DSCP

Reverse DSCP

Step 8: Load Balancing Configuration

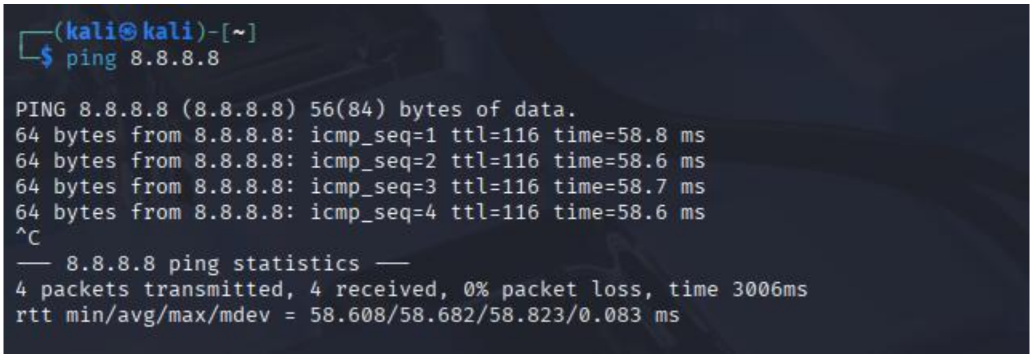
- **Mode:** Source-IP based
- **Purpose:** Distribute traffic across WAN links evenly while keeping sessions consistent per source IP.
- Configured in GUI (or optionally CLI for mode selection).



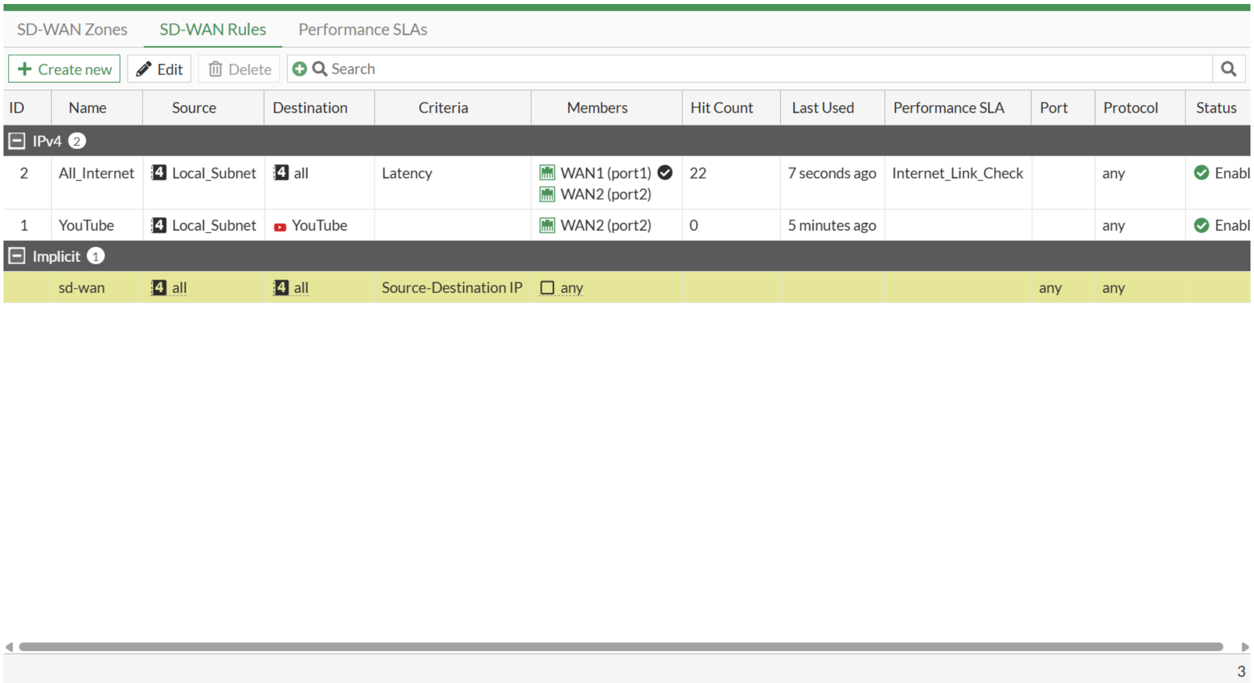
```
FGVMEVFURBQ-CY94 # config system sdwan

FGVMEVFURBQ-CY94 (sdwan) # set load-balance-mode source-ip-based

FGVMEVFURBQ-CY94 (sdwan) # end

FGVMEVFURBQ-CY94 #
```

Step 9: Testing & Monitoring

- Observed SD-WAN member status:
    - WAN1: Up
    - WAN2: Down
- Tested traffic routing for YouTube and VoIP services to verify SLA rules and best-quality routing.
- Verified failover functionality by simulating WAN link failure.
- Monitored latency, jitter, and packet loss via SD-WAN Monitor dashboard.



```
┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=58.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=58.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=58.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=58.6 ms
^C
── 8.8.8.8 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 58.608/58.682/58.823/0.083 ms
```



ID	Name	Source	Destination	Criteria	Members	Hit Count	Last Used	Performance SLA	Port	Protocol	Status
IPv4 2											
2	All_Internet	Local_Subnet	all	Latency	WAN1 (port1) ✓ WAN2 (port2)	22	7 seconds ago	Internet_Link_Check		any	✓ Enabl
1	YouTube	Local_Subnet	YouTube		WAN2 (port2)	0	5 minutes ago			any	✓ Enabl
Implicit 1											
	sd-wan	all	all	Source-Destination IP	□ any				any	any	

Conclusion

The SD-WAN implementation provides:

- Intelligent routing and application-aware traffic steering.
- Automatic failover for uninterrupted connectivity.
- Efficient utilization of all WAN links with load balancing.
- Real-time performance monitoring for proactive network management.

Mohab Nasser