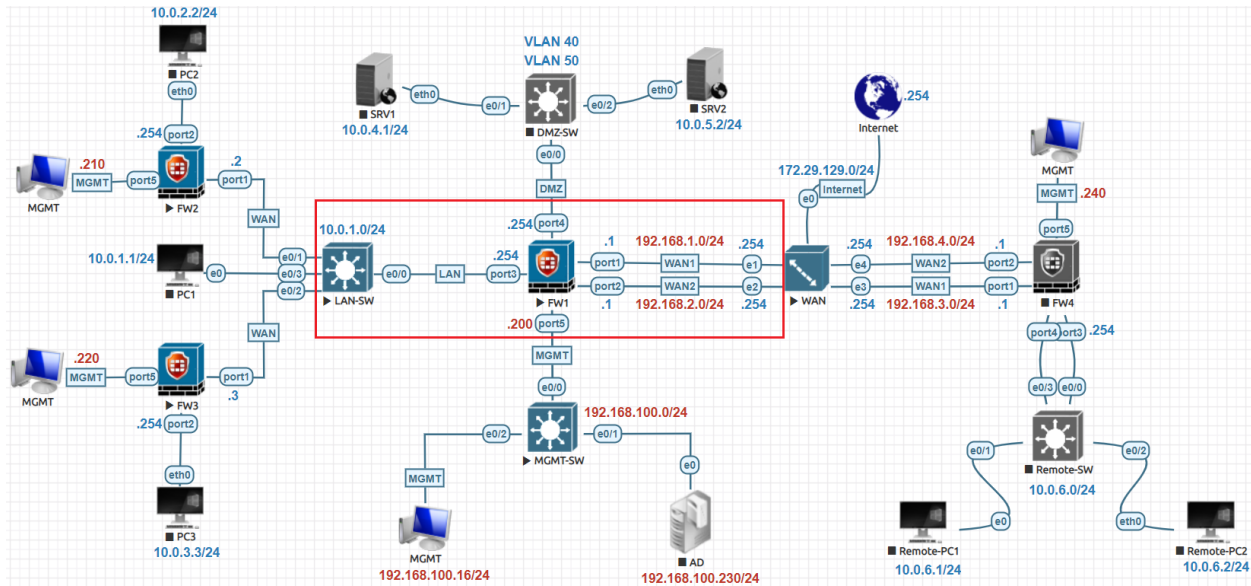
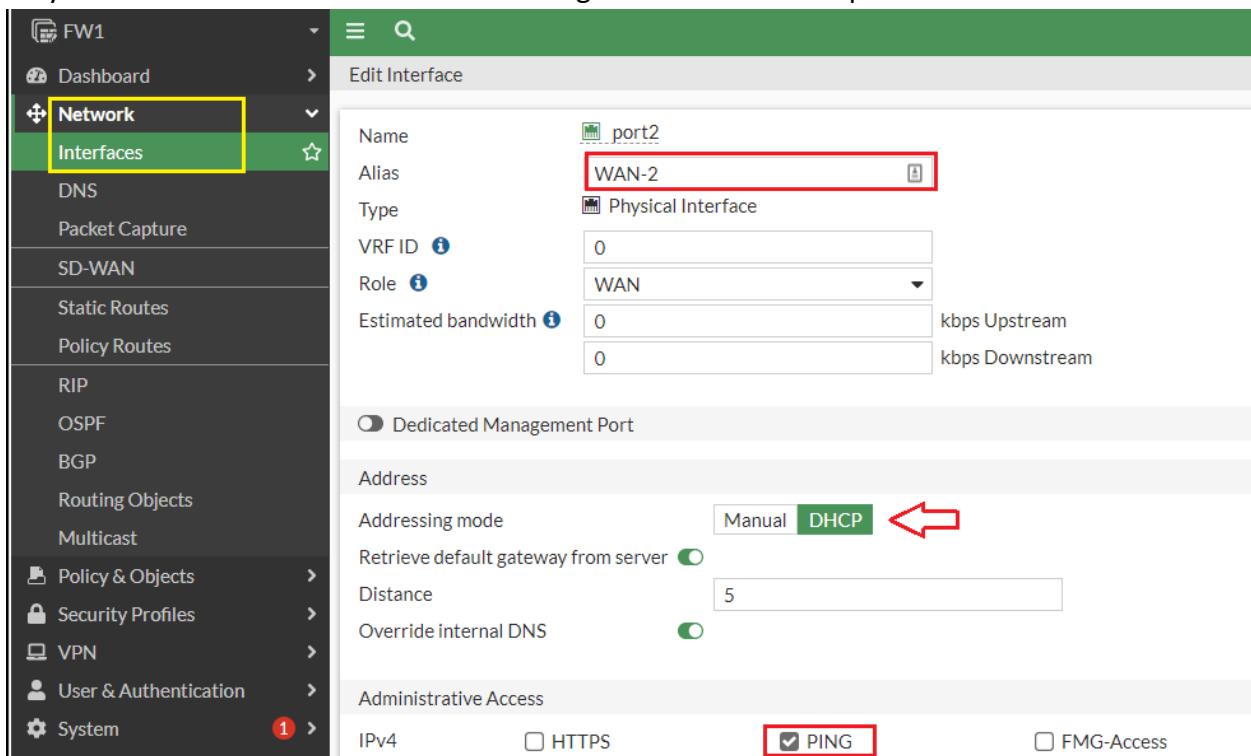


Policy Routing Lab:



Configure Interface:

Go to **Network>Interfaces** select **port2** Click **Edit** in **Alias** type **WAN-2**, change the Address Mode to **Manual** type **IP/Netmask 192.168.2.102/24**, in **Administrative access** uncheck everything only checked **PING** leave all the rest of configuration default and press **OK** button.



Default Route Configuration:

To create a new default route, go to **Network > Static Routes** and create a static route for ISP-2. Set Destination to **Subnet** and leave the destination IP address set to **0.0.0.0/0.0.0.0**. Set Gateway to the IP address provided by your ISP and Interface to the Internet-facing interface in my case **192.168.2.254** which the Gateway. Set the Interface to the **WAN-2** interface. Press **OK** to Save the changes.

The screenshot shows the 'New Static Route' configuration window. The 'Destination' is set to 'Subnet' with the value '0.0.0.0/0.0.0.0'. The 'Gateway Address' is set to 'Specify' with the value '192.168.2.254'. The 'Interface' is set to 'WAN-2 (port2)'. The 'Administrative Distance' is set to '10'. The 'Status' is 'Enabled'. A red arrow points to the 'OK' button.

Finally, now we have two default Route for equal Cost Multi-Path available.

Destination	Gateway IP	Interface	Status
0.0.0.0/0	192.168.1.254	WAN-1 (port1)	Enabled
10.0.2.0/24	10.0.1.2	LAN (port3)	Enabled
10.0.3.0/24	10.0.1.3	LAN (port3)	Enabled
0.0.0.0/0	192.168.2.254	WAN-2 (port2)	Enabled

```
FW1 # get router info routing-table static
Routing table for VRF=0
S* 0.0.0.0/0 [5/0] via 192.168.1.254, port1, [1/0]
    [5/0] via 192.168.2.254, port2, [1/0]
S   10.0.2.0/24 [10/0] via 10.0.1.2, port3, [1/0]
S   10.0.3.0/24 [10/0] via 10.0.1.3, port3, [1/0]
```

Change Equal Cost Multi-Path Mode

```
FW1 # config system settings
FW1 (settings) # set v4-ecmp-mode weight-based
FW1 (settings) # end
```

Creating a Policy:

To create a new policy, go to **Policy & Objects > Firewall Policy**. Give the policy a **Name** that indicates that the policy will be for traffic to the Internet in my case it is **Allow-All**. Set the **Incoming Interface** to **LAN** and the **Outgoing Interface** to **WAN-2**. Set Source, Destination Address, Schedule, and Services, as required in this case All. Ensure the **Action** is set to **ACCEPT**. Turn on **NAT** and select **Use Outgoing Interface Address**.

The screenshot shows the 'Edit Policy' configuration window for a firewall policy. The policy name is 'Allow LAN to Internet WAN2'. The incoming interface is 'LAN (port3)' and the outgoing interface is 'WAN-2 (port2)'. The source and destination are both set to 'all'. The schedule is 'always' and the service is 'ALL'. The action is set to 'ACCEPT'. The 'NAT' option is checked under 'Firewall / Network Options'.

Finally, we have two Firewall policy one for LAN to WAN-1 and second for LAN to WAN-2.

The screenshot shows the 'Firewall Policy' list interface. The policy 'Allow LAN to Internet WAN2' is highlighted, showing its configuration: Name: Allow LAN to Internet WAN2, Source: all, Destination: all, Schedule: always, Service: ALL, Action: ACCEPT.

Name	Source	Destination	Schedule	Service	Action
DMZ-Zone → WAN-1 (port1)					
LAN (port3) → WAN-1 (port1)					
Allow Internet Access for LAN	all	all	always	ALL	ACCEPT
LAN (port3) → WAN-2 (port2)					
Allow LAN to Internet WAN2	all	all	always	ALL	ACCEPT
Implicit					

Policy Routes:

Navigate to **Network>Policy Routes > Create New** let's create a policy route to send PC3 as a source 10.0.3.3 all traffic to next hop or gateway 192.168.2.254 which is WAN-2.

FW1

Dashboard

Network

Interfaces

DNS

Packet Capture

SD-WAN

Static Routes

Policy Routes

RIP

OSPF

BGP

Routing Objects

Multicast

Policy & Objects

Security Profiles

VPN

User & Authentication

System

Security Fabric

Log & Report

Edit Routing Policy

If incoming traffic matches:

Incoming interface: LAN (port3)

Source Address: IP/Netmask: 10.0.3.3/255.255.255.255

Addresses: all

Destination Address: IP/Netmask:

Addresses: all

Internet service:

Protocol: TCP UDP SCTP **ANY** Specify

Type of service: 0x00 Bit Mask: 0x00

Then:

Action: **Forward Traffic** Stop Policy Routing

Outgoing interface: **WAN-2 (port2)**

Gateway address: 192.168.2.254

Comments: Write a comment... 0/255

Status: **Enabled** Disabled

FW1

Dashboard

Network

Interfaces

DNS

Packet Capture

SD-WAN

Static Routes

Policy Routes

+ Create New Edit Delete Search

Seq.#	Incoming Interface	Outgoing Interface	Source	Destination
1	LAN (port3)	WAN-2 (port2)	10.0.3.3/255.255.255.255	all
2	LAN (port3)	WAN-1 (port1)	10.0.2.2/255.255.255.255	all

Verification and Testing:

Let's traceroute from PC3 as you can see the traffic is passing through WAN-2 gateway.

```
PC3
Applications Places System Thu May 5, 21:25
root@PC3: ~
File Edit View Search Terminal Help
root@PC3:~# traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 10.0.3.254 (10.0.3.254) 5.312 ms 5.298 ms 5.285 ms
 2 10.0.1.254 (10.0.1.254) 7.480 ms 7.481 ms 7.471 ms
 3 192.168.2.254 (192.168.2.254) 9.216 ms 9.217 ms 9.208 ms
 4 172.29.129.254 (172.29.129.254) 9.224 ms 10.302 ms 10.414 ms
 5 192.168.100.1 (192.168.100.1) 10.410 ms 10.402 ms 12.266 ms
 6 84-235-86-35.saudi.net.sa (84.235.86.35) 17.483 ms 13.551 ms 13.635 ms
 7 10.188.193.68 (10.188.193.68) 11.513 ms 13.954 ms 10.188.193.80 (10.188.193.80) 11.043 ms
 8 10.188.193.21 (10.188.193.21) 20.897 ms 10.188.193.43 (10.188.193.43) 13.748 ms 10.188.193.21 (10.188.193.21) 13.855 ms
 9 10.188.195.73 (10.188.195.73) 27.292 ms 10.188.199.44 (10.188.199.44) 29.093 ms 29.096 ms
10 72.14.197.0 (72.14.197.0) 77.447 ms 74.125.147.0 (74.125.147.0) 77.097 ms 74.125.50.128 (74.125.50.128) 82.467 ms
11 * * 108.170.252.241 (108.170.252.241) 89.389 ms
12 dns.google (8.8.8.8) 89.007 ms 89.295 ms 142.250.224.95 (142.250.224.95)
```

Let's check Forward Traffic for the given Source 10.0.3.3 Destination Interface is WAN-2.

Date/Time	Source	Device	Destination Interface	Destination
19 seconds ago	10.0.3.3	FortiGate-VM64-KVM	WAN-2 (port2)	1.1.1.1 (one.one.one.one)
19 seconds ago	10.0.3.3	FortiGate-VM64-KVM	WAN-2 (port2)	1.1.1.1 (one.one.one.one)
19 seconds ago	10.0.3.3	FortiGate-VM64-KVM	WAN-2 (port2)	1.1.1.1 (one.one.one.one)
Minute ago	10.0.3.3	FortiGate-VM64-KVM	WAN-2 (port2)	8.8.8.8 (dns.google)
Minute ago	10.0.3.3	FortiGate-VM64-KVM	WAN-2 (port2)	8.8.8.8 (dns.google)
Minute ago	10.0.3.3	FortiGate-VM64-KVM	WAN-2 (port2)	8.8.8.8 (dns.google)
3 minutes ago	10.0.3.3	FortiGate-VM64-KVM	WAN-1 (port1)	35.160.82.219 (push.services)

Verify through Fortigate Firewall FW1 CLI there is hit counts for ID=1 which is first policy.

```
FW1
FW1 # diagnose firewall proute list
list route policy info(vf=root):

id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=5 dp
ort=0-65535 path(1) oif=4(port2) gwy=192.168.2.254
destination(1): 0.0.0.0-255.255.255.255
source wildcard(1): 10.0.3.3/255.255.255.255
hit_count=6 last_used=2022-05-06 04:52:13
```

Policy Routes:

Navigate to **Network>Policy Routes > Create New** let's create a policy route to send PC2 as a source 10.0.2.2 all traffic to next hop or gateway 192.168.1.254 which is WAN-1.

The screenshot shows the configuration for a new routing policy. The 'Incoming interface' is set to LAN (port3). The 'Source Address' is 10.0.2.2/255.255.255.255. The 'Destination Address' is set to 'all'. The 'Protocol' is set to 'ANY'. The 'Action' is 'Forward Traffic'. The 'Outgoing interface' is set to WAN-1 (port1) and the 'Gateway address' is 192.168.1.254. The status is 'Enabled'.

Seq.#	Incoming Interface	Outgoing Interface	Source
1	LAN (port3)	WAN-2 (port2)	10.0.3.3/255.255.255.255
2	LAN (port3)	WAN-1 (port1)	10.0.2.2/255.255.255.255

Verification and Testing:

Let's traceroute from PC2 as you can see the traffic is passing through WAN-1 gateway.

```

root@PC2:~# traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 10.0.2.254 (10.0.2.254) 1.662 ms 2.242 ms 2.239 ms
 2 10.0.1.254 (10.0.1.254) 2.232 ms 7.781 ms 8.031 ms
 3 192.168.1.254 (192.168.1.254) 8.032 ms 8.323 ms 8.320 ms
 4 172.29.129.254 (172.29.129.254) 10.526 ms 10.527 ms 10.522 ms
 5 192.168.100.1 (192.168.100.1) 10.516 ms 10.509 ms 10.502 ms
 6 84-235-86-35.saudi.net.sa (84.235.86.35) 17.872 ms 8.331 ms 18.801 ms
 7 10.188.193.68 (10.188.193.68) 21.064 ms 18.715 ms 10.188.193.80 (10.188.193.80) 21.013 ms
 8 10.188.193.23 (10.188.193.23) 19.013 ms 10.188.193.21 (10.188.193.21) 19.027 ms 10.188.193.23 (10.188.193.23) 19.004 ms
 9 10.188.195.45 (10.188.195.45) 30.066 ms 10.188.199.44 (10.188.199.44) 45.237 ms 10.188.195.73 (10.188.195.73) 34.653 ms
10 74.125.147.0 (74.125.147.0) 87.511 ms 87.519 ms 72.14.211.158 (72.14.211.158) 92.661 ms
11 74.125.245.225 (74.125.245.225) 93.704 ms * 108.170.245.1 (108.170.245.1) 97.207 ms
12 dns.google (8.8.8.8) 68.835 ms 142.251.78.81 (142.251.78.81) 68.793 ms dns.google (8.8.8.8) 68.527 ms
root@PC2:~#
    
```

Seq.#	Incoming Interface	Outgoing Interface	Source	Destination	Hit Count
1	LAN (port3)	WAN-2 (port2)	10.0.3.3/255.255.255.255	all	1,140
2	LAN (port3)	WAN-1 (port1)	10.0.2.2/255.255.255.255	all	92

Date/Time	Source	Device	Destination Interface	Destination
2 seconds ago	10.0.2.2	FortiGate-VM64-KVM	WAN-1 (port1)	1.1.1.1 (one.one.one.one)
22 seconds ago	10.0.2.2	FortiGate-VM64-KVM	WAN-1 (port1)	8.8.8.8 (dns.google)
22 seconds ago	10.0.2.2	FortiGate-VM64-KVM	WAN-1 (port1)	8.8.8.8 (dns.google)
22 seconds ago	10.0.2.2	FortiGate-VM64-KVM	WAN-1 (port1)	8.8.8.8 (dns.google)
22 seconds ago	10.0.2.2	FortiGate-VM64-KVM	WAN-1 (port1)	8.8.8.8 (dns.google)
22 seconds ago	10.0.2.2	FortiGate-VM64-KVM	WAN-1 (port1)	8.8.8.8 (dns.google)
22 seconds ago	10.0.2.2	FortiGate-VM64-KVM	WAN-1 (port1)	8.8.8.8 (dns.google)

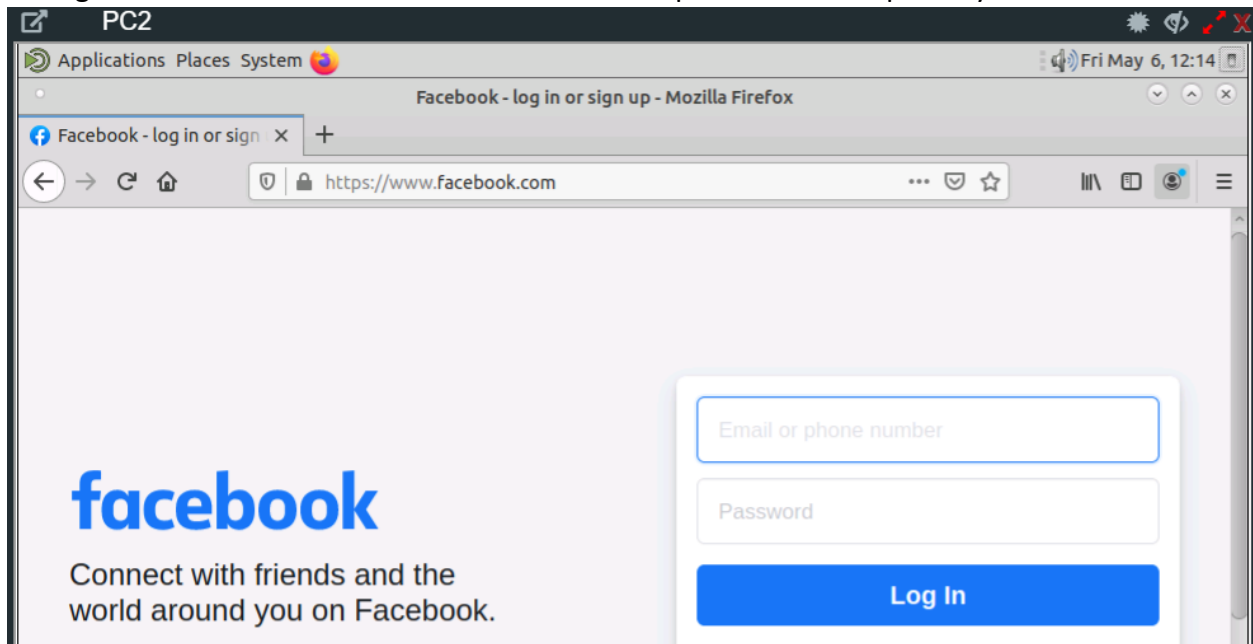
Verify through Fortigate Firewall FW1 CLI there is hit counts for ID=2 which is second policy.

```
FW1 # diagnose firewall proute list
list route policy info(vf=root):

id=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=5 dp
ort=0-65535 path(1) oif=4(port2) gwy=192.168.2.254
destination(1): 0.0.0.0-255.255.255.255
source wildcard(1): 10.0.3.3/255.255.255.255
hit_count=6 last_used=2022-05-06 04:52:13

id=2 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=5 dp
ort=0-65535 path(1) oif=3(port1) gwy=192.168.1.254
destination(1): 0.0.0.0-255.255.255.255
source wildcard(1): 10.0.2.2/255.255.255.255
hit_count=3 last_used=2022-05-06 04:49:24
```

Let's generate some traffic from Internal LAN PC2 open a browser open any website.



After generate the traffic the hit count increase for policy number 2 which is ID=2.

```
FW1 #
FW1 # diagnose firewall proute list 2
list route policy info(vf=root):

id=2 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=5 dp
ort=0-65535 path(1) oif=3(port1) gwy=192.168.1.254
destination(1): 0.0.0.0-255.255.255.255
source wildcard(1): 10.0.2.2/255.255.255.255
hit_count=62 last_used=2022-05-06 05:13:33

FW1 # █
```