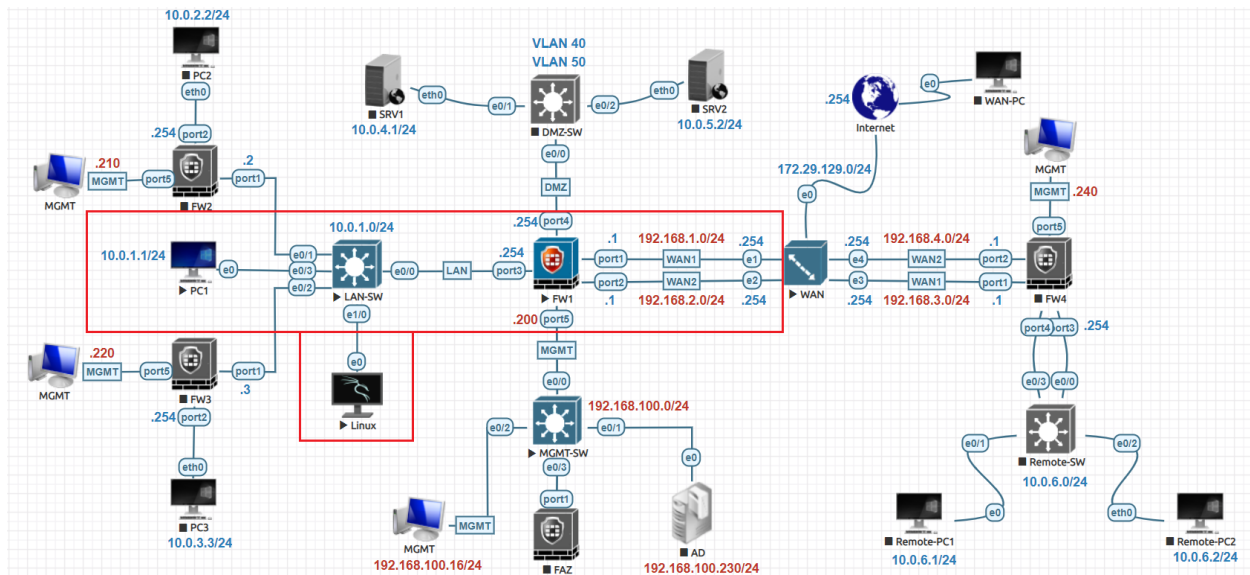
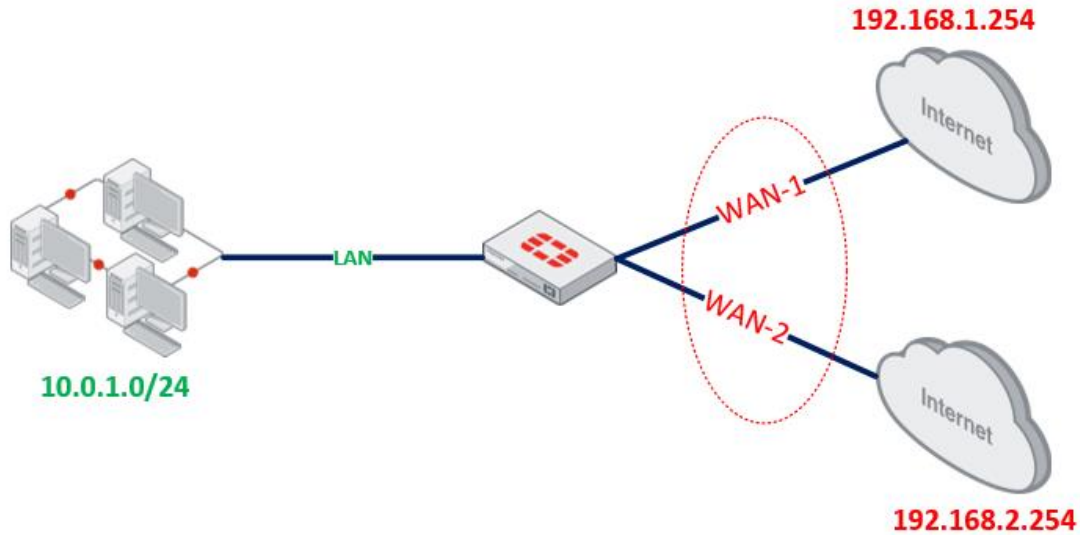


ECMP (Equal-Cost Multi-Path Routing) Lab:

With FortiGate Firewall you can make multiple WAN Lines (Internet Lines) redundant and load balance communication. Here, we will confirm the Load Balancing operation by ECMP (Equal Cost Multiple Path) for two Internet Lines.



WAN-1 Gateway	192.168.1.254
WAN-2 Gateway	192.168.2.254
WAN-1 Port	Port1
WAN-2 Port	Port2
Server to check	8.8.8.8
Protocols to use	Ping

Default Routes:

Create two default routes for the redundant Internet connections, both the default static routes have to be active in the routing table. Set the same Distance and Priority of both the routes. To configure these routes in the GUI, go to **Network -> Static Routes** and create two default routes.

FW1

Dashboard

Network

Interfaces

DNS

Packet Capture

SD-WAN

Static Routes

Policy Routes

RIP

OSPF

BGP

Routing Objects

Multicast

Edit Static Route

Automatic gateway retrieval

Destination **Subnet** Internet Service

0.0.0.0/0.0.0.0

Gateway Address **Dynamic** Specify 192.168.1.254

Interface WAN-1 (port1)

Administrative Distance 10

Comments Write a comment... 0/255

Status Enabled Disabled

Advanced Options

Priority 1

FW1

Dashboard

Network

Interfaces

DNS

Packet Capture

SD-WAN

Static Routes

Policy Routes

RIP

OSPF

BGP

Routing Objects

Multicast

Edit Static Route

Automatic gateway retrieval

Destination **Subnet** Internet Service

0.0.0.0/0.0.0.0

Gateway Address 192.168.2.254

Interface WAN-2 (port2)

Administrative Distance 10

Comments Write a comment... 0/255

Status Enabled Disabled

Advanced Options

Priority 1

A default route is set for each Internet Line. You can check the routing table with the CLI command **get router info routing-table static**.

```
CLI Console (1)
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]
FW1 #
```

You can also verify from GUI go to **Dashboard >Network** click on **Static & Dynamic Routing**.

Network	Gateway IP	Interfaces	Distance	Type	Metric	Prior...
10.0.1.0/24	0.0.0.0	LAN (port3)	0	Connected	0	0
10.0.4.0/24	0.0.0.0	VLAN-40 (VLAN-40)	0	Connected	0	0
10.0.5.0/24	0.0.0.0	VLAN-50 (VLAN-50)	0	Connected	0	0
192.168.1.0/24	0.0.0.0	WAN-1 (port1)	0	Connected	0	0
192.168.2.0/24	0.0.0.0	WAN-2 (port2)	0	Connected	0	0
192.168.114.0/24	0.0.0.0	MGMT (port5)	0	Connected	0	0
0.0.0.0/0	192.168.1.254	WAN-1 (port1)	5	Static	0	1
0.0.0.0/0	192.168.2.254	WAN-2 (port2)	5	Static	0	1

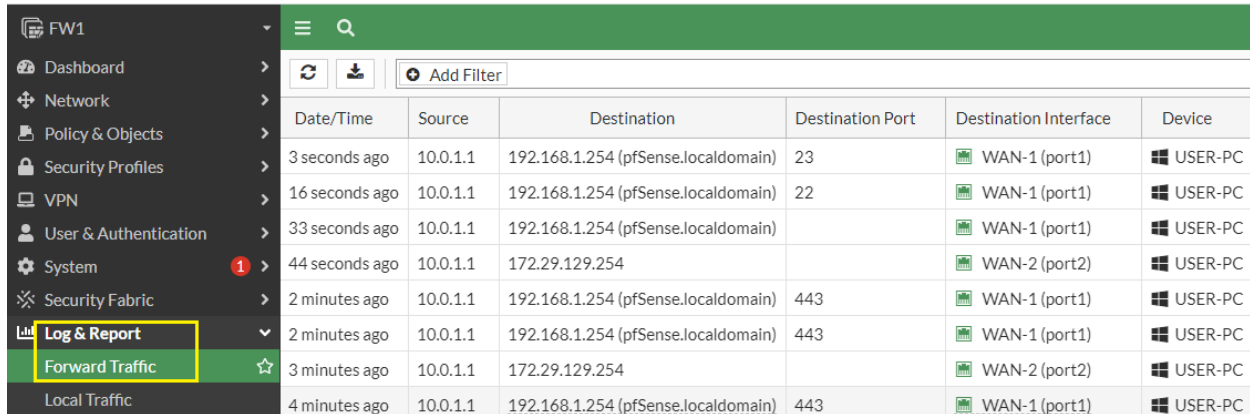
Firewall Policy:

Set a policy to allow all communication from LAN to WAN1 and LAN to WAN2 respectively.

ID	Name	From	To	Source	Hit Count
9	Allow-DNS	LAN (port3)	WAN-1 (port1) WAN-2 (port2)	all	557
1	Allow LAN-to-WAN	LAN (port3)	WAN-1 (port1) WAN-2 (port2)	all	0

Test and Verification:

Access multiple sites such as Google and Yahoo from your device and check **Log & Report > Forwarding Traffic**. You will see that all sites are using the **WAN1** primary Line. As FortiGate's default, load balancing to multiple routes (ECMP) distributes the **Source IP Address**. Therefore, the same source uses the same route (in this case, for the primary Line of the WAN1).

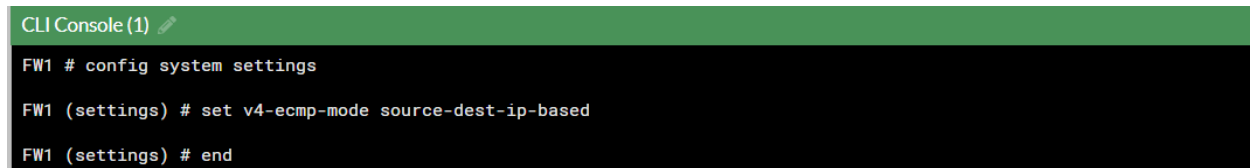


Date/Time	Source	Destination	Destination Port	Destination Interface	Device
3 seconds ago	10.0.1.1	192.168.1.254 (pfSense.localdomain)	23	WAN-1 (port1)	USER-PC
16 seconds ago	10.0.1.1	192.168.1.254 (pfSense.localdomain)	22	WAN-1 (port1)	USER-PC
33 seconds ago	10.0.1.1	192.168.1.254 (pfSense.localdomain)		WAN-1 (port1)	USER-PC
44 seconds ago	10.0.1.1	172.29.129.254		WAN-2 (port2)	USER-PC
2 minutes ago	10.0.1.1	192.168.1.254 (pfSense.localdomain)	443	WAN-1 (port1)	USER-PC
2 minutes ago	10.0.1.1	192.168.1.254 (pfSense.localdomain)	443	WAN-1 (port1)	USER-PC
3 minutes ago	10.0.1.1	172.29.129.254		WAN-2 (port2)	USER-PC
4 minutes ago	10.0.1.1	192.168.1.254 (pfSense.localdomain)	443	WAN-1 (port1)	USER-PC

Let's change Load Balancing (ECMP) which should be performed based on the pair of source IP address and destination IP address. Settings are made using the CLI.

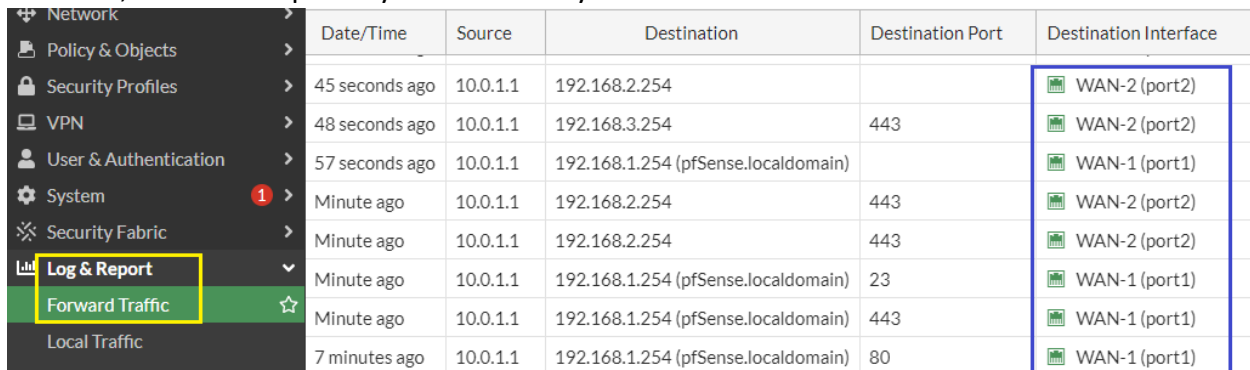
FW1 Change ECMP

```
config system settings
set v4-ecmp-mode source-dest-ip-based
end
```



```
CLI Console (1)
FW1 # config system settings
FW1 (settings) # set v4-ecmp-mode source-dest-ip-based
FW1 (settings) # end
```

Access multiple sites such as Google and Yahoo again from the terminal and check the **Log & Report > Forwarding Traffic**. The source IP address is fixed, but the destination IP address is different, so both the primary and secondary WAN lines are used.



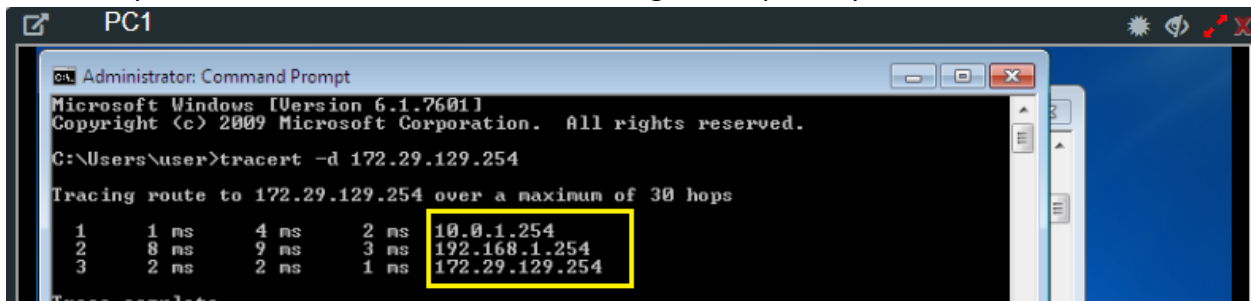
Date/Time	Source	Destination	Destination Port	Destination Interface	Device
45 seconds ago	10.0.1.1	192.168.2.254		WAN-2 (port2)	
48 seconds ago	10.0.1.1	192.168.3.254	443	WAN-2 (port2)	
57 seconds ago	10.0.1.1	192.168.1.254 (pfSense.localdomain)		WAN-1 (port1)	
Minute ago	10.0.1.1	192.168.2.254	443	WAN-2 (port2)	
Minute ago	10.0.1.1	192.168.2.254	443	WAN-2 (port2)	
Minute ago	10.0.1.1	192.168.1.254 (pfSense.localdomain)	23	WAN-1 (port1)	
Minute ago	10.0.1.1	192.168.1.254 (pfSense.localdomain)	443	WAN-1 (port1)	
7 minutes ago	10.0.1.1	192.168.1.254 (pfSense.localdomain)	80	WAN-1 (port1)	

Health Link Monitor:

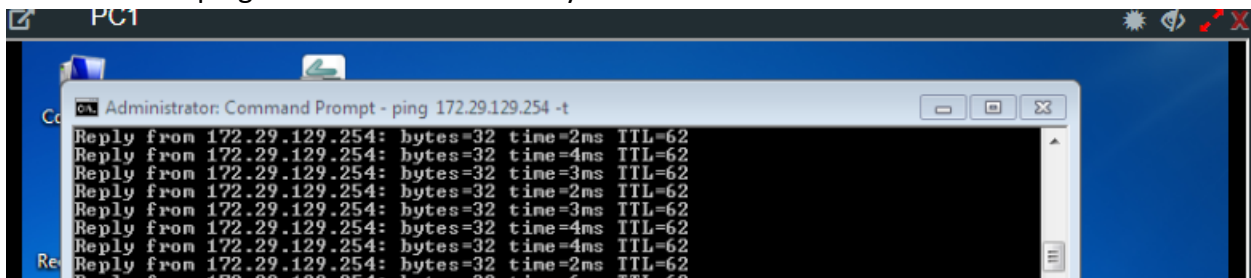
Let's set up the Health Link Monitor and configure ping servers CLI Only. The following will ping a server of your choice, and if it stops receiving replies at the set rate, it will pull the static route from the routing table and the secondary connection will be used.

FW1 CLI Configuration
<pre>config system link-monitor edit WAN1 set srcintf port1 set server 8.8.8.8 set protocol ping set gateway-ip 192.168.1.254 set source-ip 0.0.0.0 set interval 500 set failtime 5 set recoverytime 5 set ha-priority 1 set update-cascade-interface enable set update-static-route enable set status enable end</pre>
<pre>config system link-monitor edit WAN2 set srcintf port2 set server 8.8.8.8 set protocol ping set gateway-ip 192.168.2.254 set source-ip 0.0.0.0 set interval 500 set failtime 5 set recoverytime 5 set ha-priority 1 set update-cascade-interface enable set update-static-route enable set status enable end</pre>
<pre>diagnose sys link-monitor status</pre>

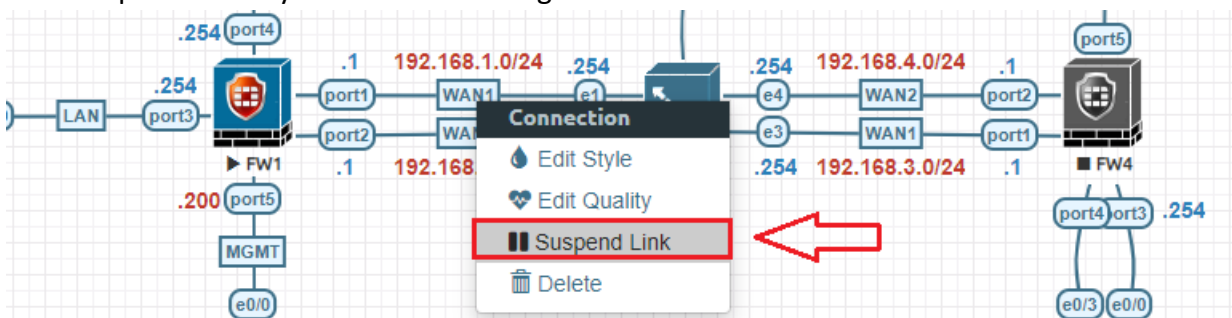
Let's verify traceroute from internal PC1, it is using WAN1 primary link for communication.



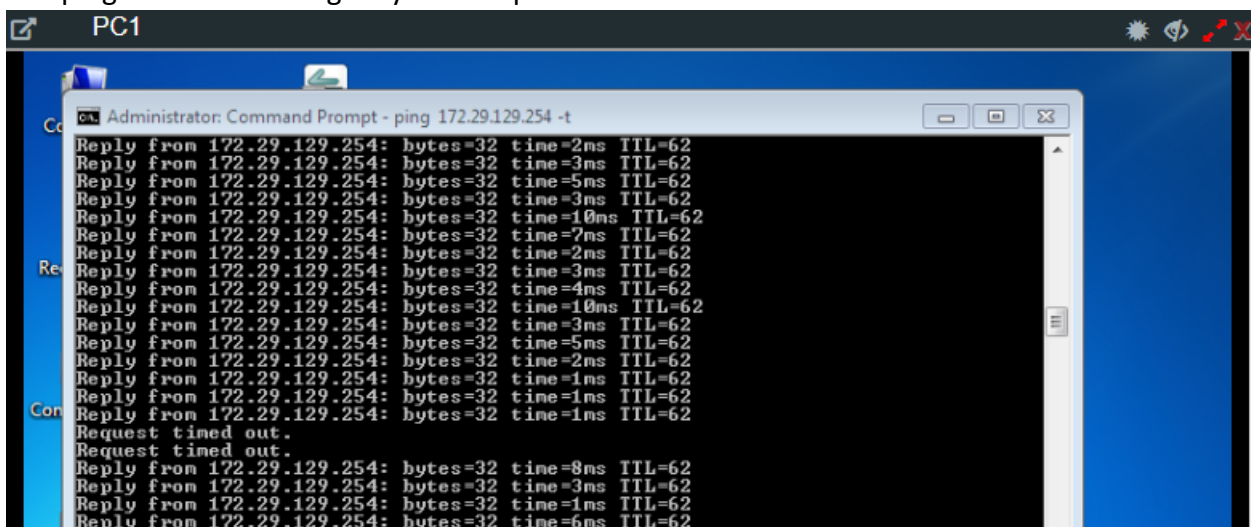
Start continue ping from Internal PC1 to any external IP Address such as 8.8.8.8.



Let's Suspend Primary WAN1 Link to bring them down.



The ping is still continuing only few drops.



Let's check the traceroute again this time it is using WAN2 secondary internet Link.

```

PC1
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\user>tracert -d 172.29.129.254

Tracing route to 172.29.129.254 over a maximum of 30 hops

  1    1 ms    4 ms    2 ms  10.0.1.254
  2    8 ms    9 ms    3 ms  192.168.1.254
  3    2 ms    2 ms    1 ms  172.29.129.254

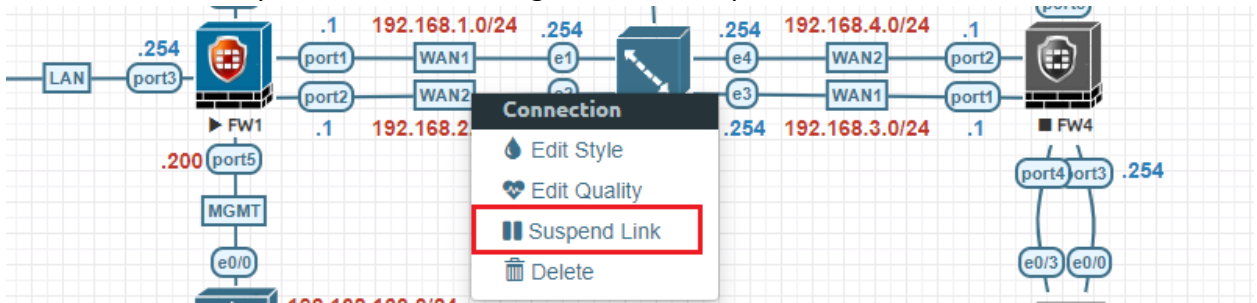
Trace complete.

C:\Users\user>tracert -d 172.29.129.254

Tracing route to 172.29.129.254 over a maximum of 30 hops

  1    2 ms    2 ms    1 ms  10.0.1.254
  2    3 ms    4 ms    8 ms  192.168.2.254
  3    2 ms    3 ms    3 ms  172.29.129.254
    
```

Let's enable Primary WAN1 link and bring down and suspend WAN2 Link.



The ping is still continuing only few drops.

```

PC1
Administrator: Command Prompt - ping 172.29.129.254 -t

Reply from 172.29.129.254: bytes=32 time=2ms TTL=62
Reply from 172.29.129.254: bytes=32 time=3ms TTL=62
Reply from 172.29.129.254: bytes=32 time=5ms TTL=62
Reply from 172.29.129.254: bytes=32 time=3ms TTL=62
Reply from 172.29.129.254: bytes=32 time=10ms TTL=62
Reply from 172.29.129.254: bytes=32 time=7ms TTL=62
Reply from 172.29.129.254: bytes=32 time=2ms TTL=62
Reply from 172.29.129.254: bytes=32 time=3ms TTL=62
Reply from 172.29.129.254: bytes=32 time=4ms TTL=62
Reply from 172.29.129.254: bytes=32 time=10ms TTL=62
Reply from 172.29.129.254: bytes=32 time=3ms TTL=62
Reply from 172.29.129.254: bytes=32 time=5ms TTL=62
Reply from 172.29.129.254: bytes=32 time=2ms TTL=62
Reply from 172.29.129.254: bytes=32 time=1ms TTL=62
Reply from 172.29.129.254: bytes=32 time=1ms TTL=62
Reply from 172.29.129.254: bytes=32 time=1ms TTL=62
Request timed out.
Request timed out.
Reply from 172.29.129.254: bytes=32 time=8ms TTL=62
Reply from 172.29.129.254: bytes=32 time=3ms TTL=62
    
```

Let's check the traceroute again this time it is using WAN1 Primary Internet Link again.

```

Administrator: Command Prompt
3      2 ms    3 ms    3 ms    172.29.129.254
Trace complete.
C:\Users\user>tracert -d 172.29.129.254
Tracing route to 172.29.129.254 over a maximum of 30 hops
  0  1 ms    1 ms    1 ms    10.0.1.254
  1  2 ms    3 ms    3 ms    192.168.2.254
  2  8 ms    8 ms    9 ms    172.29.129.254
Trace complete.
C:\Users\user>tracert -d 172.29.129.254
Tracing route to 172.29.129.254 over a maximum of 30 hops
  0  1 ms    1 ms    1 ms    10.0.1.254
  1  2 ms    2 ms    4 ms    192.168.1.254
  2  3 ms    1 ms    1 ms    172.29.129.254

```

When WAN1 link goes down, navigate to system event logs as below and verify the logs
 FortiGate GUI -> Log and Report > Events > System Events.

	Date/Time	Level	Message	Log Description
	13 seconds ago	■■■■■	Performance statistics: average CPU: 7, memory: 77, concu...	System performance ...
	15 seconds ago	■■■■■	Administrator admin logged out from jsconsole	Admin logout success...
	Minute ago	■■■■■	ha state is changed from 0 to 1	Link monitor status
	Minute ago	■■■■■	Link Monitor changed state from alive to dead, protocol: ping.	Link monitor status
	Minute ago	■■■■■	Link monitor: Interface port2 was turned down	Interface status chan...
	3 minutes ago	■■■■■	interface port1 gets a DHCP lease, ip:192.168.1.102, mask:2...	DHCP client lease gra...
	3 minutes ago	■■■■■	interface port1 gets a DHCP lease, ip:192.168.1.102, mask:2...	DHCP client lease gra...
	3 minutes ago	■■■■■	Static route on interface port1 may be added by link-monito...	Routing information c...
	3 minutes ago	■■■■■	ha state is changed from 1 to 0	Link monitor status
	3 minutes ago	■■■■■	Link Monitor changed state from dead to alive, protocol: ping.	Link monitor status

When one link is down verifying the Routing table through CLI it will show only one route.

```

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]

```

Network	Gateway IP	Interfaces	Distance	Type	Metric	Priority
10.0.1.0/24	0.0.0.0	LAN (port3)	0	Connected	0	0
10.0.4.0/24	0.0.0.0	VLAN-40 (VLAN-40)	0	Connected	0	0
10.0.5.0/24	0.0.0.0	VLAN-50 (VLAN-50)	0	Connected	0	0
192.168.1.0/24	0.0.0.0	WAN-1 (port1)	0	Connected	0	0
192.168.114.0/24	0.0.0.0	MGMT (port5)	0	Connected	0	0
0.0.0.0/0	192.168.1.254	WAN-1 (port1)	5	Static	0	1