# Contents

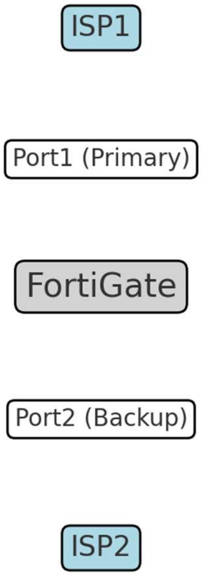
## The objective of the Lab

To configure Local-FortiGate with two internet interfaces where:
- Port1 serves as the primary internet link.
- Port2 serves as the backup internet link.
- The backup (port2) will only be used when the primary (port1) is down.

This is achieved using two default routes with different administrative distances.

## Topology

Description:
- Local-FortiGate:
  - Port1: Primary internet link (ISP1).
  - Port2: Backup internet link (ISP2).



## Components Used

1. FortiGate firewall.
2. Two ISPs:
   - ISP1 connected to port1.
   - ISP2 connected to port2.
3. FortiOS 7.x or higher.

## Steps of the Lab

**Verify the Routing Configuration**

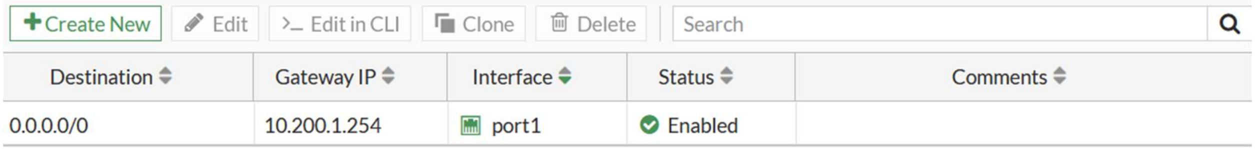
You will verify the existing routing configuration on Local-FortiGate.

**To verify the routing configuration**

2. Connect to the Local-FortiGate GUI, and then log in

3. Click **Network** > **Static Routes**.

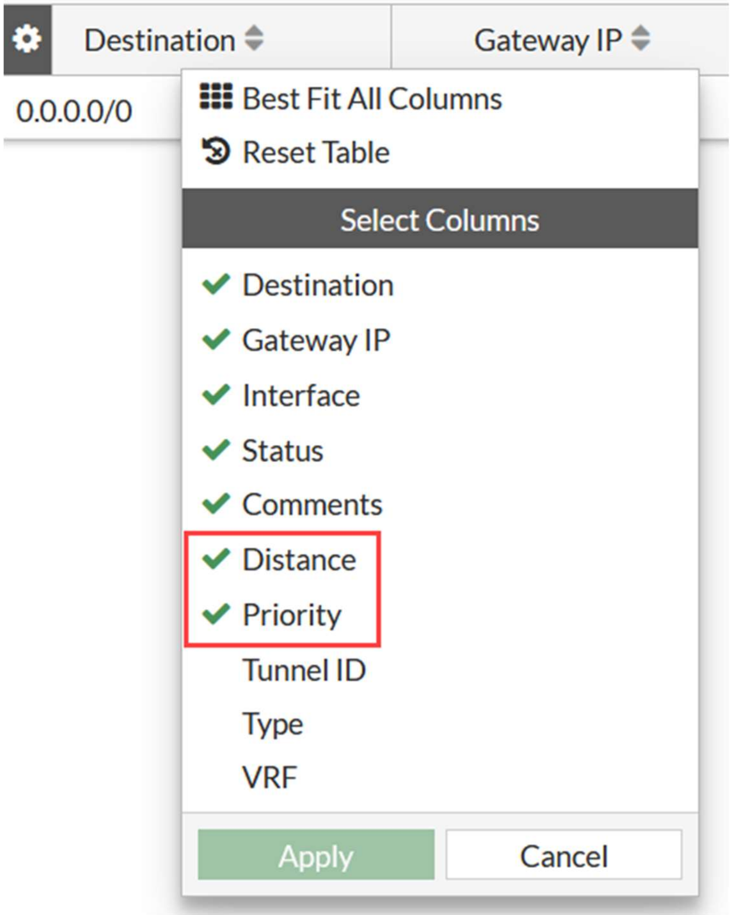
3. Verify the existing default route for **port1**.



| Destination | Gateway IP | Interface | Status | Comments |
|---|---|---|---|---|
| 0.0.0.0/0 | 10.200.1.254 | port1 | ✓ Enabled | |

4. Right-click any of the column headers to open the context-sensitive menu.

5. In the **Select Columns** section, select **Distance** and **Priority**, and then click **Apply**.



The **Distance** and **Priority** columns appear on the GUI.

Note that, by default, static routes have a **Distance** value of 10 and a **Priority** value of 1.

**Configure a Second Default Route**

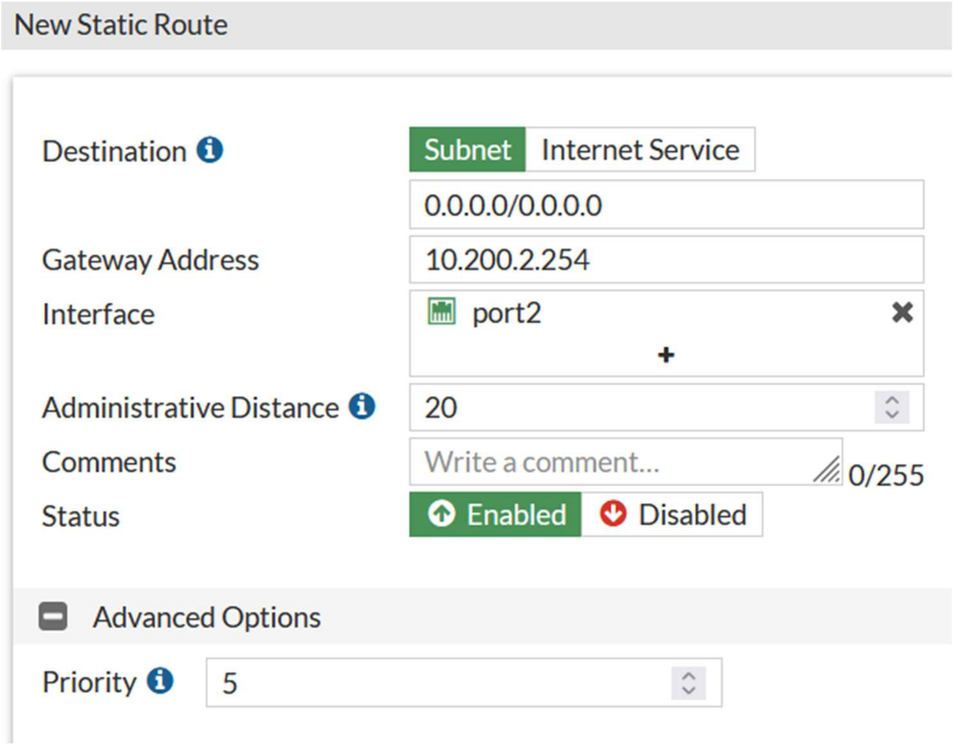
You will create a second default route using the port2 interface. To make sure this second default route remains the standby route, you will assign it a higher administrative distance than the first default route.

**To configure a second default route**

1. Continuing on the Local-FortiGate GUI, click **Network** > **Static Routes**.
2. Click **Create New**.
3. Configure the following settings:

| **Field** | **Value** |
|---|---|
| Gateway Address | 10.200.2.254 |
| Interface | port2 |
| Administrative Distance | 20 |

4. Click **+** to expand the **Advanced Options** section.
5. In the **Priority** field, type 5.



New Static Route

Destination: Subnet | Internet Service

0.0.0.0/0.0.0.0

Gateway Address: 10.200.2.254

Interface: port2

Administrative Distance: 20

Comments: Write a comment... 0/255

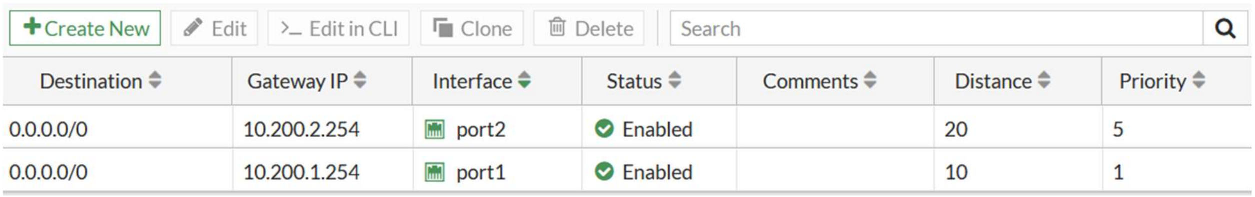
Status: Enabled | Disabled

Advanced Options

Priority: 5

6. Click **OK**.

FortiGate adds a second default route.



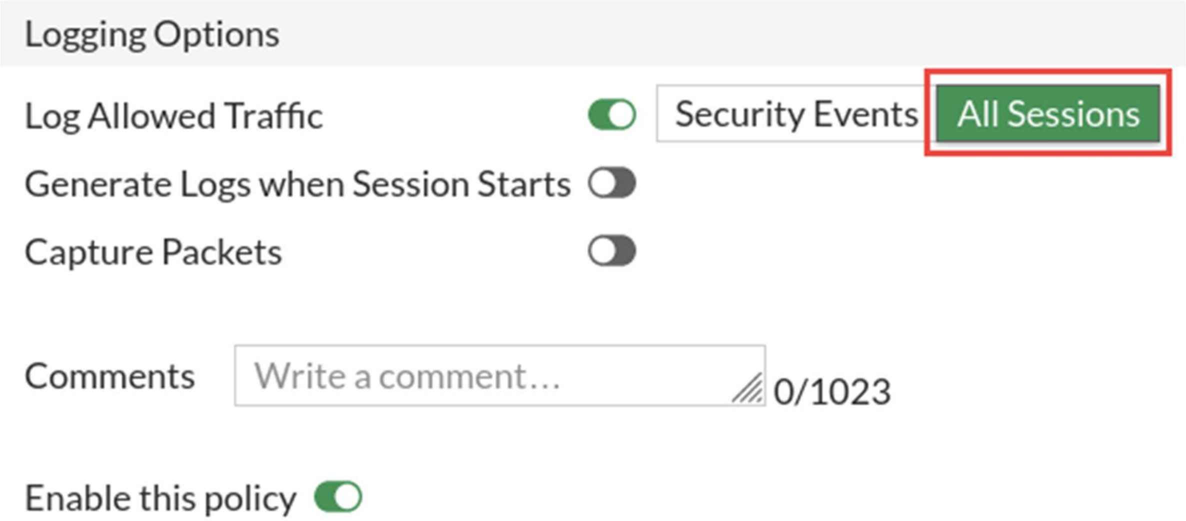
| Destination | Gateway IP | Interface | Status | Comments | Distance | Priority |
|---|---|---|---|---|---|---|
| 0.0.0.0/0 | 10.200.2.254 | port2 | ✓ Enabled | | 20 | 5 |
| 0.0.0.0/0 | 10.200.1.254 | port1 | ✓ Enabled | | 10 | 1 |

**Configure the Firewall Policies**

You will modify the existing **Full_Access** firewall policy to log all sessions. You will also create a second firewall policy to allow traffic through the secondary interface.

**To configure the firewall policies**

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Double-click the existing **Full_Access** policy to edit it.
3. Enable **Log Allowed Traffic**, and then select **All Sessions**.



Logging Options

Log Allowed Traffic ● Security Events | All Sessions

Generate Logs when Session Starts ○

Capture Packets ○

Comments Write a comment... 0/1023

Enable this policy ●

4. Click **OK**.
5. Click **Create New**.
6. Configure a second firewall policy with the following settings:

| **Field** | **Value** |
|---|---|
| Name | Backup_Access |
| Incoming Interface | port3 |
| Outgoing Interface | port2 |
| Source | LOCAL_SUBNET |

| **Field** | **Value** |
|---|---|
| Destination | all |
| Schedule | always |
| Service | ALL |
| Log Allowed Traffic | All Sessions |

7. Click **OK**.

**View the Routing Table**

The Local-FortiGate configuration now has two default routes with different distances. You will view the routing table to see which route was installed in the routing table and which route was installed in the routing table database.

**To view the routing table**

1. On the Local-FortiGate CLI, log in with the username admin and password password.
2. Enter the following command to list the routing table entries:

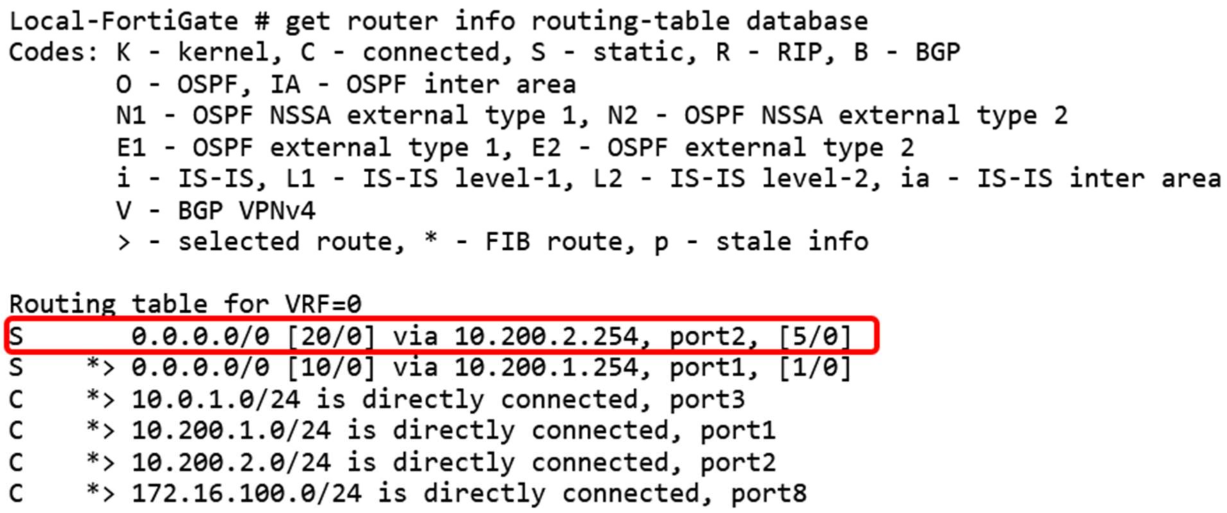
```
get router info routing-table all
```

Note that the second default route is not listed.

3. Enter the following command to list the routing table database entries:

```
get router info routing-table database
```

4. Confirm that the second default route is listed as inactive.



```
Local-FortiGate # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S       0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S    *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C    *> 10.0.1.0/24 is directly connected, port3
C    *> 10.200.1.0/24 is directly connected, port1
C    *> 10.200.2.0/24 is directly connected, port2
C    *> 172.16.100.0/24 is directly connected, port8
```

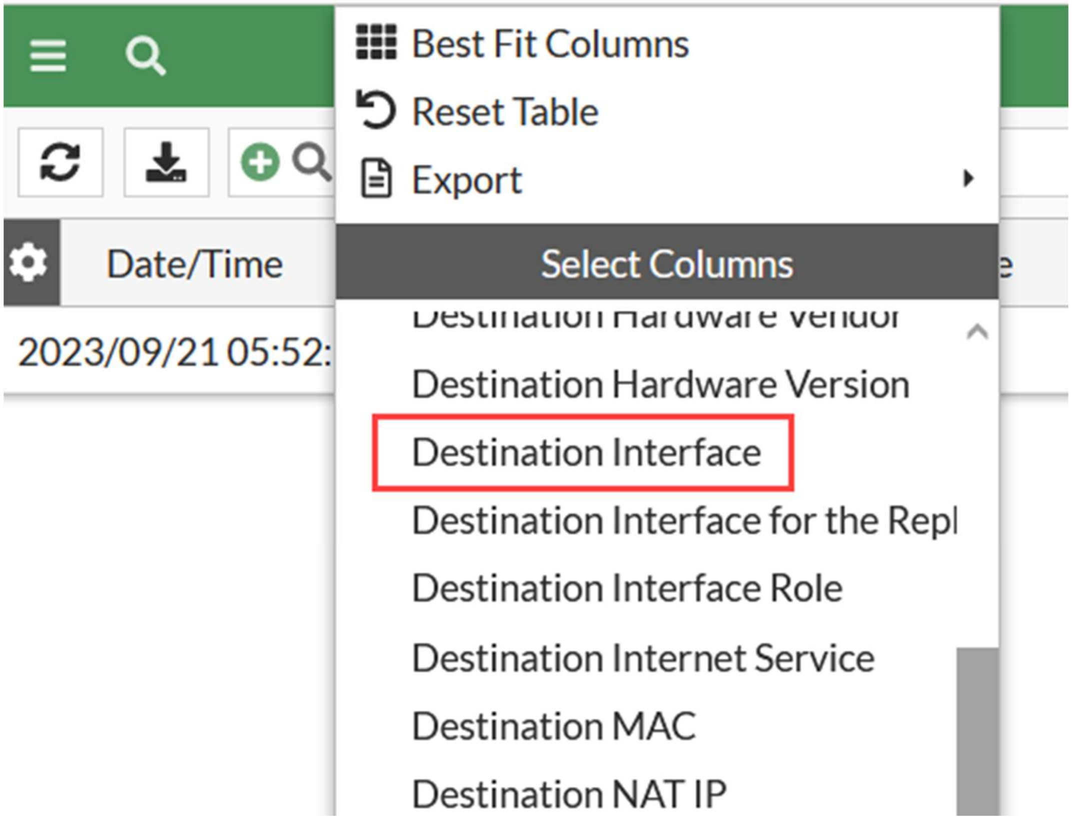
5. Close the Local-FortiGate CLI session.

### Testing the Lab

First, you will access various websites and use the **Forward Traffic** logs to verify that the port1 route is being used. Next, you will force a failover by reconfiguring the port1 interface setting and bringing the interface down. You will then generate some more traffic, and use the **Forward Traffic** logs to verify that the port2 route is being used.

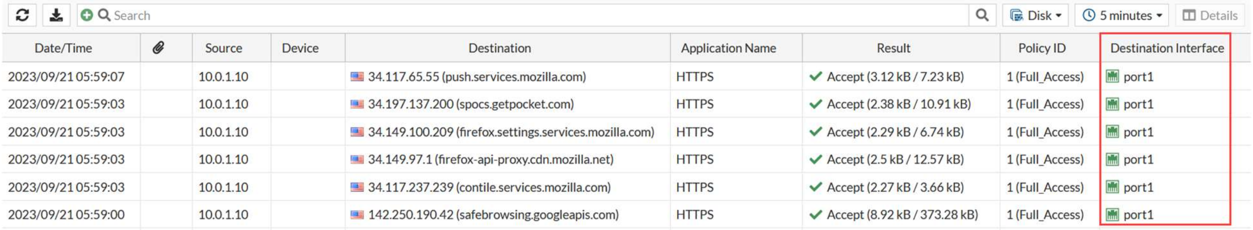
**To confirm the port1 route is the primary route**

1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.
2. Right-click any of the column headers to open the context-sensitive menu.
3. In the **Select Columns** section, select **Destination Interface**.


Best Fit Columns
Reset Table
Export
Date/Time
2023/09/21 05:52:
Select Columns
Destination Hardware Vendor
Destination Hardware Version
Destination Interface
Destination Interface for the Repl
Destination Interface Role
Destination Internet Service
Destination MAC
Destination NAT IP

4. Scroll down in the context-sensitive menu, and then click **Apply**.

The **Destination Interface** column is displayed.

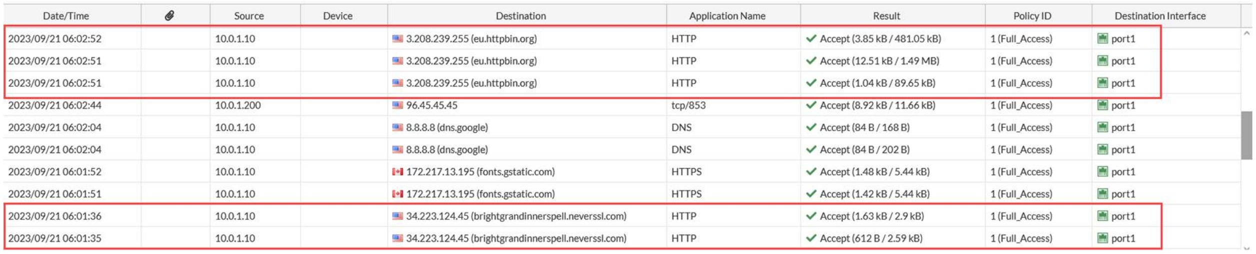


| Date/Time | 🔗 | Source | Device | Destination | Application Name | Result | Policy ID | Destination Interface |
|---|---|---|---|---|---|---|---|---|
| 2023/09/21 05:59:07 | | 10.0.1.10 | | 34.117.65.55 (push.services.mozilla.com) | HTTPS | ✓ Accept (3.12 kB / 7.23 kB) | 1 (Full_Access) | port1 |
| 2023/09/21 05:59:03 | | 10.0.1.10 | | 34.197.137.200 (spocs.getpocket.com) | HTTPS | ✓ Accept (2.38 kB / 10.91 kB) | 1 (Full_Access) | port1 |
| 2023/09/21 05:59:03 | | 10.0.1.10 | | 34.149.100.209 (firefox.settings.services.mozilla.com) | HTTPS | ✓ Accept (2.29 kB / 6.74 kB) | 1 (Full_Access) | port1 |
| 2023/09/21 05:59:03 | | 10.0.1.10 | | 34.149.97.1 (firefox-api-proxy.cdn.mozilla.net) | HTTPS | ✓ Accept (2.5 kB / 12.57 kB) | 1 (Full_Access) | port1 |
| 2023/09/21 05:59:03 | | 10.0.1.10 | | 34.117.237.239 (contile.services.mozilla.com) | HTTPS | ✓ Accept (2.27 kB / 3.66 kB) | 1 (Full_Access) | port1 |
| 2023/09/21 05:59:00 | | 10.0.1.10 | | 142.250.190.42 (safebrowsing.googleapis.com) | HTTPS | ✓ Accept (8.92 kB / 373.28 kB) | 1 (Full_Access) | port1 |

5. On the Local-Client VM, in the browser, open a few new tabs, and then visit a few websites, such as:

- http://neverssl.com
- http://eu.httpbin.org

6. On the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.
7. Click the refresh icon.
8. Locate the relevant log entries for the websites you accessed, and then verify that the **Destination Interface** indicates **port1**.



| Date/Time | 🔗 | Source | Device | Destination | Application Name | Result | Policy ID | Destination Interface |
|---|---|---|---|---|---|---|---|---|
| 2023/09/21 06:02:52 | | 10.0.1.10 | | 3.208.239.255 (eu.httpbin.org) | HTTP | ✓ Accept (3.85 kB / 481.05 kB) | 1 (Full_Access) | port1 |
| 2023/09/21 06:02:51 | | 10.0.1.10 | | 3.208.239.255 (eu.httpbin.org) | HTTP | ✓ Accept (12.51 kB / 1.49 MB) | 1 (Full_Access) | port1 |
| 2023/09/21 06:02:51 | | 10.0.1.10 | | 3.208.239.255 (eu.httpbin.org) | HTTP | ✓ Accept (1.04 kB / 89.65 kB) | 1 (Full_Access) | port1 |
| 2023/09/21 06:02:44 | | 10.0.1.200 | | 96.45.45.45 | tcp/853 | ✓ Accept (8.92 kB / 11.66 kB) | 1 (Full_Access) | port1 |
| 2023/09/21 06:02:04 | | 10.0.1.10 | | 8.8.8.8 (dns.google) | DNS | ✓ Accept (84 B / 168 B) | 1 (Full_Access) | port1 |
| 2023/09/21 06:02:04 | | 10.0.1.10 | | 8.8.8.8 (dns.google) | DNS | ✓ Accept (84 B / 202 B) | 1 (Full_Access) | port1 |
| 2023/09/21 06:01:52 | | 10.0.1.10 | | 172.217.13.195 (fonts.gstatic.com) | HTTPS | ✓ Accept (1.48 kB / 5.44 kB) | 1 (Full_Access) | port1 |
| 2023/09/21 06:01:51 | | 10.0.1.10 | | 172.217.13.195 (fonts.gstatic.com) | HTTPS | ✓ Accept (1.42 kB / 5.44 kB) | 1 (Full_Access) | port1 |
| 2023/09/21 06:01:36 | | 10.0.1.10 | | 34.223.124.45 (brightgrandinnerspell.neverssl.com) | HTTP | ✓ Accept (1.63 kB / 2.9 kB) | 1 (Full_Access) | port1 |
| 2023/09/21 06:01:35 | | 10.0.1.10 | | 34.223.124.45 (brightgrandinnerspell.neverssl.com) | HTTP | ✓ Accept (612 B / 2.59 kB) | 1 (Full_Access) | port1 |

This verifies that the port1 route is currently the route in use.

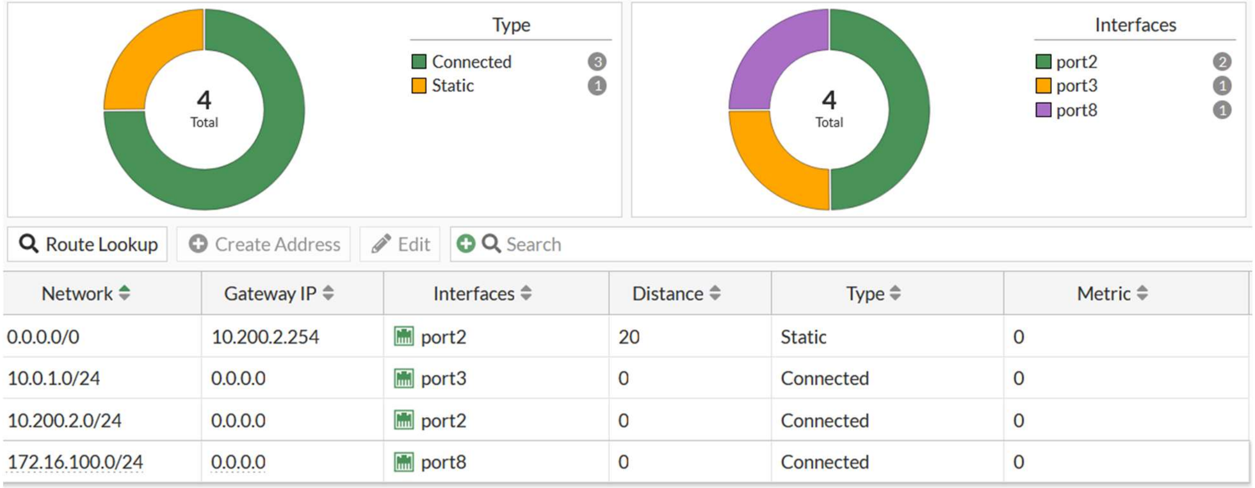
### To force the failover

1. Continuing on the Local-FortiGate GUI, click **Network** > **Interfaces**.
2. Double-click the **port1** interface to edit it.
3. In the **Miscellaneous** section, click **Disabled** as the status.
4. Click **OK**.

The port1 internet connection is now down, and FortiGate removes the corresponding route from the routing table.

### To verify the route change

1. Continuing on the Local-FortiGate GUI, click **Dashboard** > **Network**, and then click **Static & Dynamic Routing** to expand it to full screen.
2. In the routing table, verify that the **port2** route replaced the **port1** route.



| Network | Gateway IP | Interfaces | Distance | Type | Metric |
|---|---|---|---|---|---|
| 0.0.0.0/0 | 10.200.2.254 | port2 | 20 | Static | 0 |
| 10.0.1.0/24 | 0.0.0.0 | port3 | 0 | Connected | 0 |
| 10.200.2.0/24 | 0.0.0.0 | port2 | 0 | Connected | 0 |
| 172.16.100.0/24 | 0.0.0.0 | port8 | 0 | Connected | 0 |

### To verify traffic logs

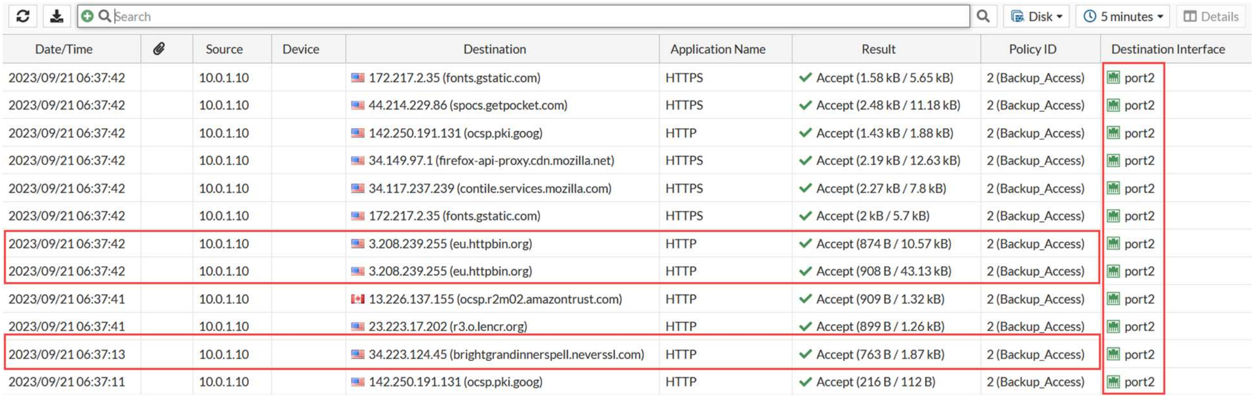
1. On the Local-Client VM, in the browser, open a few new tabs, and then visit a few websites, such as:

- http://neverssl.com

- http://eu.httpbin.org

2. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and then click **Log & Report** > **Forward Traffic**.

3. Locate the relevant log entries for the websites you accessed, and then verify that the **Destination Interface** indicates **port2**.



| Date/Time | | Source | Device | Destination | Application Name | Result | Policy ID | Destination Interface |
|---|---|---|---|---|---|---|---|---|
| 2023/09/21 06:37:42 | | 10.0.1.10 | | 172.217.2.35 (fonts.gstatic.com) | HTTPS | ✓ Accept (1.58 kB / 5.65 kB) | 2 (Backup_Access) | port2 |
| 2023/09/21 06:37:42 | | 10.0.1.10 | | 44.214.229.86 (spocs.getpocket.com) | HTTPS | ✓ Accept (2.48 kB / 11.18 kB) | 2 (Backup_Access) | port2 |
| 2023/09/21 06:37:42 | | 10.0.1.10 | | 142.250.191.131 (ocsp.pki.goog) | HTTP | ✓ Accept (1.43 kB / 1.88 kB) | 2 (Backup_Access) | port2 |
| 2023/09/21 06:37:42 | | 10.0.1.10 | | 34.149.97.1 (firefox-api-proxy.cdn.mozilla.net) | HTTPS | ✓ Accept (2.19 kB / 12.63 kB) | 2 (Backup_Access) | port2 |
| 2023/09/21 06:37:42 | | 10.0.1.10 | | 34.117.237.239 (contile.services.mozilla.com) | HTTPS | ✓ Accept (2.27 kB / 7.8 kB) | 2 (Backup_Access) | port2 |
| 2023/09/21 06:37:42 | | 10.0.1.10 | | 172.217.2.35 (fonts.gstatic.com) | HTTPS | ✓ Accept (2 kB / 5.7 kB) | 2 (Backup_Access) | port2 |
| 2023/09/21 06:37:42 | | 10.0.1.10 | | 3.208.239.255 (eu.httpbin.org) | HTTP | ✓ Accept (874 B / 10.57 kB) | 2 (Backup_Access) | port2 |
| 2023/09/21 06:37:42 | | 10.0.1.10 | | 3.208.239.255 (eu.httpbin.org) | HTTP | ✓ Accept (908 B / 43.13 kB) | 2 (Backup_Access) | port2 |
| 2023/09/21 06:37:41 | | 10.0.1.10 | | 13.226.137.155 (ocsp.r2m02.amazontrust.com) | HTTP | ✓ Accept (909 B / 1.32 kB) | 2 (Backup_Access) | port2 |
| 2023/09/21 06:37:41 | | 10.0.1.10 | | 23.223.17.202 (r3.o.lencr.org) | HTTP | ✓ Accept (899 B / 1.26 kB) | 2 (Backup_Access) | port2 |
| 2023/09/21 06:37:13 | | 10.0.1.10 | | 34.223.124.45 (brightgrandinnerspell.neverssl.com) | HTTP | ✓ Accept (763 B / 1.87 kB) | 2 (Backup_Access) | port2 |
| 2023/09/21 06:37:11 | | 10.0.1.10 | | 142.250.191.131 (ocsp.pki.goog) | HTTP | ✓ Accept (216 B / 112 B) | 2 (Backup_Access) | port2 |

This verifies that the Local-FortiGate is using the port2 default route.

### Restore the Routing Table

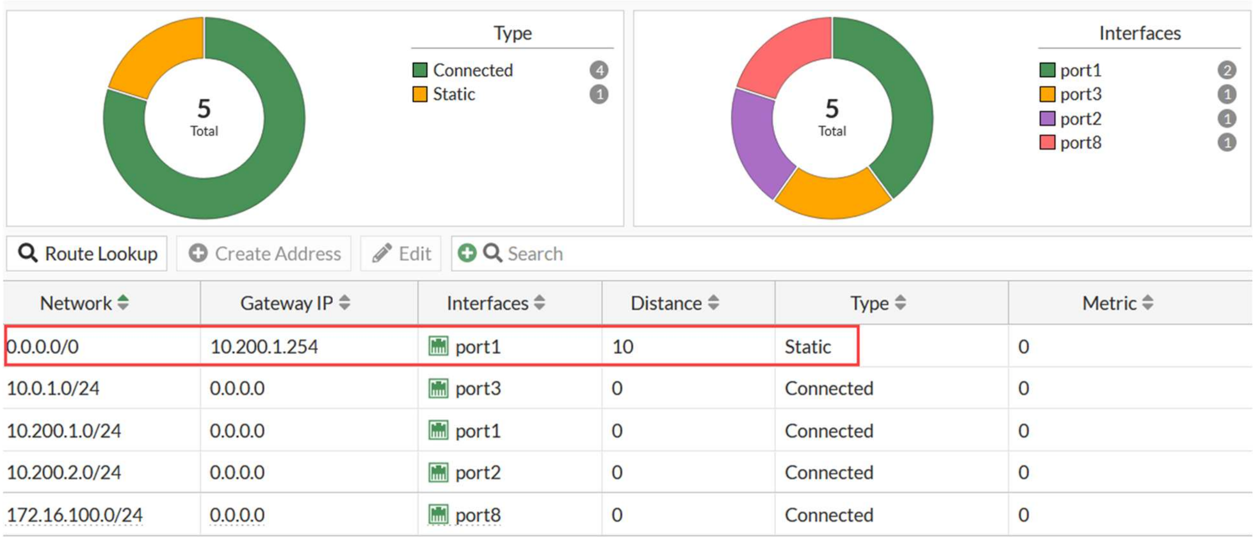
Before you begin the next exercise, you will restore the port1 interface settings and bring it up, which will restore the port1 default route as the best route in the routing table.

### To restore the port1 health monitor configuration

1. Continuing on the Local-FortiGate GUI, click **Network** > **Interfaces**.
2. Double-click the **port1** interface to edit it.
3. In the **Miscellaneous** section, click **Enabled** as the status.
4. Click **OK**.

### To verify the routing table

1. Continuing on the Local-FortiGate GUI, click **Dashboard** > **Network**, and then click **Static & Dynamic Routing** to expand it to full screen.
2. In the routing table, verify that the **port1** route replaced the **port2** route.



| Network | Gateway IP | Interfaces | Distance | Type | Metric |
|---|---|---|---|---|---|
| 0.0.0.0/0 | 10.200.1.254 | port1 | 10 | Static | 0 |
| 10.0.1.0/24 | 0.0.0.0 | port3 | 0 | Connected | 0 |
| 10.200.1.0/24 | 0.0.0.0 | port1 | 0 | Connected | 0 |
| 10.200.2.0/24 | 0.0.0.0 | port2 | 0 | Connected | 0 |
| 172.16.100.0/24 | 0.0.0.0 | port8 | 0 | Connected | 0 |

## Results

1. When port1 is active, internet traffic flows through the primary link.
2. When port1 is down, the firewall seamlessly routes traffic through the backup link.
3. Failback occurs automatically once port1 is restored.