Routing in FortiGate

After completing this document, you will be able to achieve these objectives:

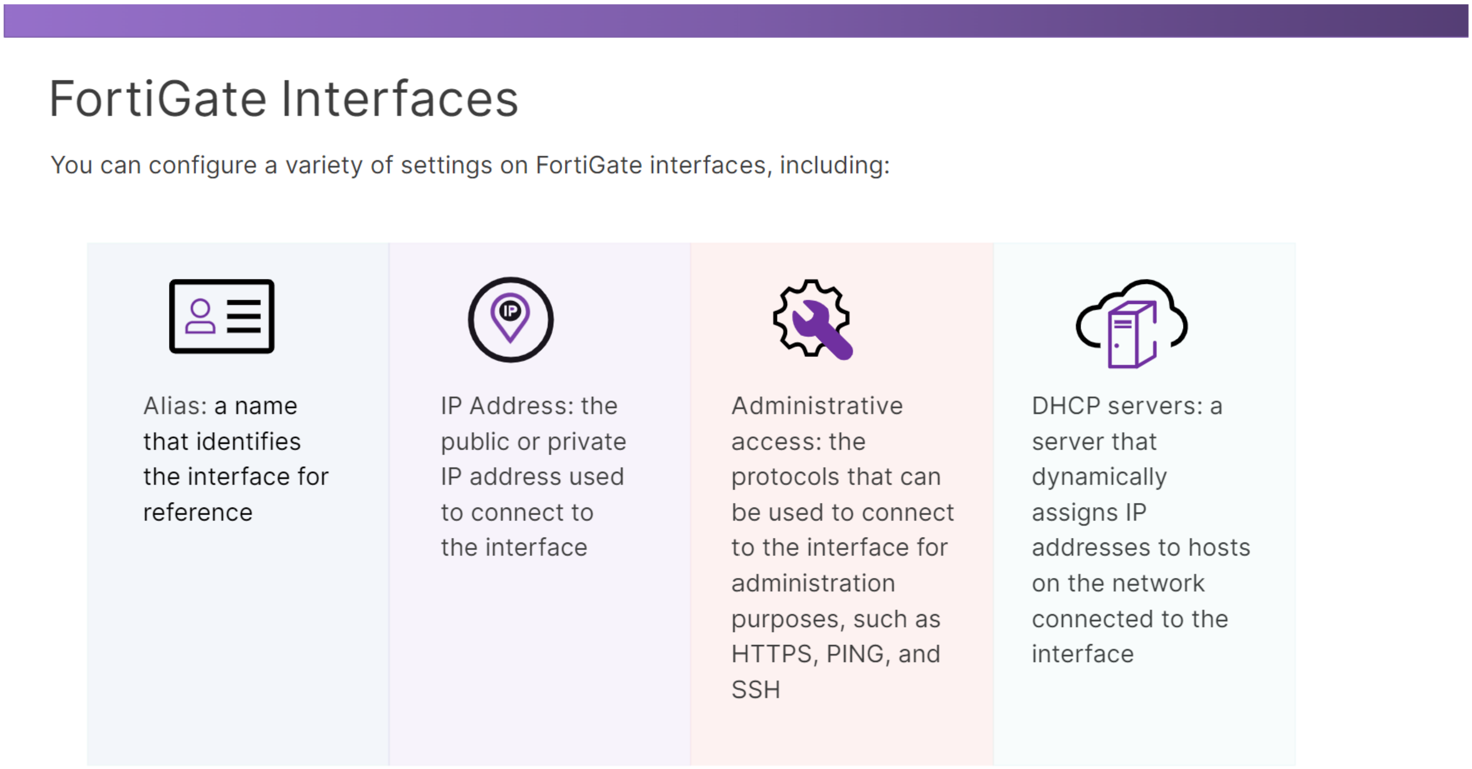
- **Configure networking interfaces**
- **Configure FortiGate as a DHCP server**
- **IP Routing**
  - **What Is IP Routing?**
  - **Route Lookup**
  - **RIB and FIB**
  - **Static Routes**
  - **Static Routes With Named Addresses**
  - **Internet Services Routing**
  - **Routing Monitor**
  - **Distance**
  - **Metric**
  - **Priority**
  - **Routing Table-CLI**
  - **Route Attributes**
  - **GUI Route Lookup Tool**
  - **Reverse Path Forwarding**
  - **ECMP**
  - **ECMP Load Balancing Algorithms**
  - **Configuring ECMP**
  - **ECMP Example**
  - **Default ECMP Algorithm vs. SD-WAN ECMP Algorithm**
- **LAB 1: Configuring Route Failover**
- **LAB 2: Configuring Equal-Cost Multi-Path Routing**

FortiGate Interfaces

Physical and virtual interfaces allow traffic to flow:

- ✓ **between internal networks,**
- ✓ **and between the internet and internal networks.**

FortiGate has options for configuring interfaces that can scale as your organization grows.



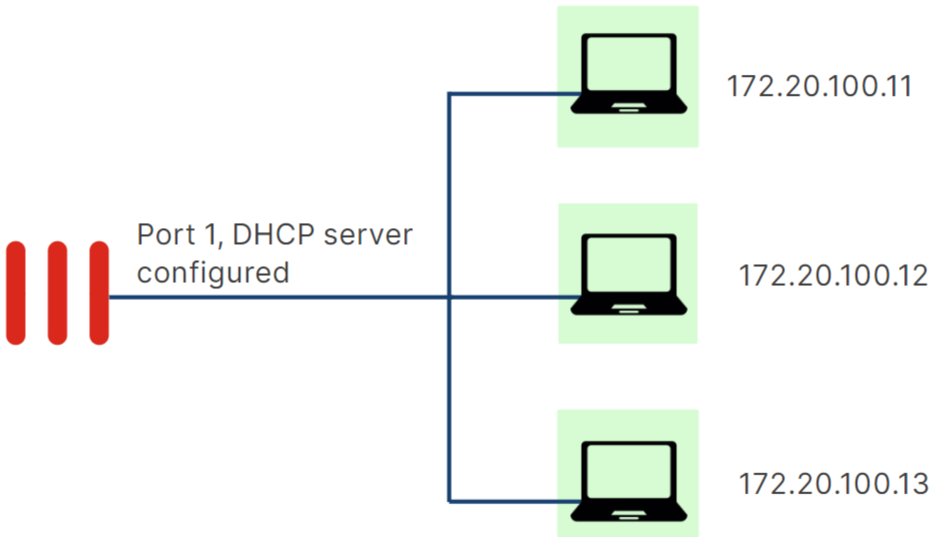
FortiGate Interfaces

You can configure a variety of settings on FortiGate interfaces, including:

Alias: a name that identifies the interface for reference	IP Address: the public or private IP address used to connect to the interface	Administrative access: the protocols that can be used to connect to the interface for administration purposes, such as HTTPS, PING, and SSH	DHCP servers: a server that dynamically assigns IP addresses to hosts on the network connected to the interface

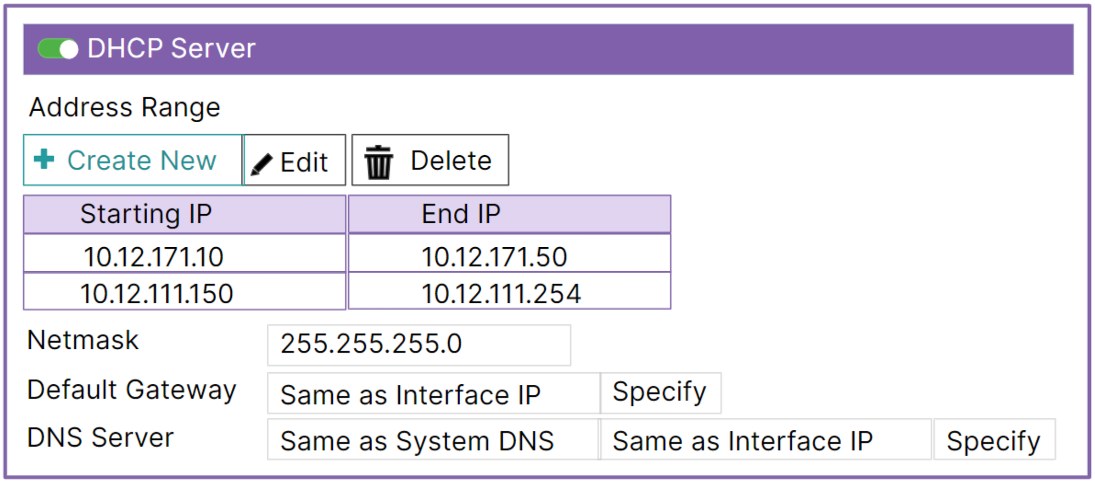
FortiGate DHCP

A DHCP server dynamically assigns IP addresses to devices on the network connected to the interface. You can configure **one or more DHCP servers on any FortiGate interface**.



A DHCP server configuration includes:

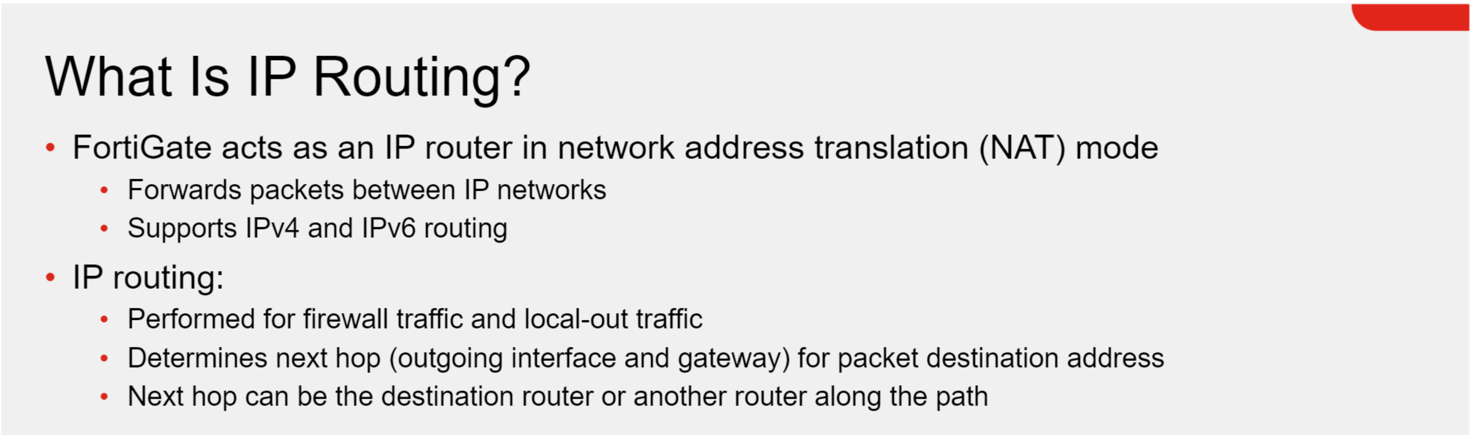
- **Address Range:** the range of IP addresses that FortiGate assigns to devices.
- **Netmask:** the netmask of the address that FortiGate assigns to devices.
- **Default Gateway:** the default gateway that FortiGate assigns to devices. By default, this gateway is the same as the interface IP address.
- **DNS Server:** the DNS server that FortiGate will assign to devices. By default, this is the same DNS server used by FortiGate.



Starting IP	End IP
10.12.171.10	10.12.171.50
10.12.111.150	10.12.111.254

Netmask	255.255.255.0		
Default Gateway	Same as Interface IP	Specify	
DNS Server	Same as System DNS	Same as Interface IP	Specify

FortiGate IP Routing



What Is IP Routing?

- FortiGate acts as an IP router in network address translation (NAT) mode
  - Forwards packets between IP networks
  - Supports IPv4 and IPv6 routing
- IP routing:
  - Performed for firewall traffic and local-out traffic
  - Determines next hop (outgoing interface and gateway) for packet destination address
  - Next hop can be the destination router or another router along the path

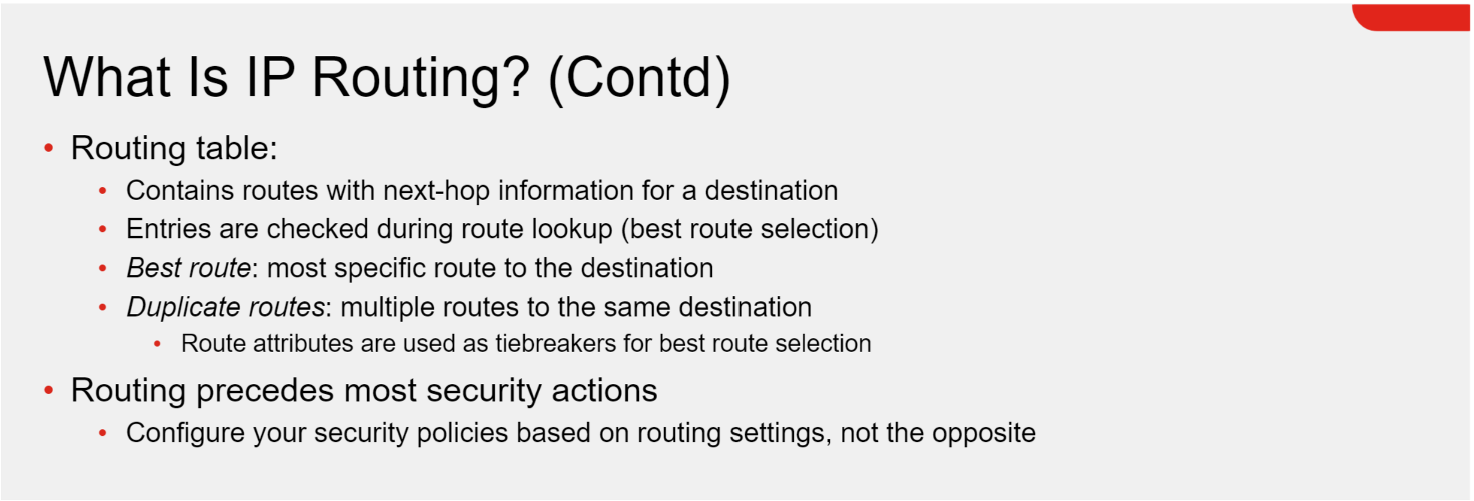
When FortiGate operates in **NAT mode**—the default operation mode—FortiGate behaves as an **IP router**. An IP router is a device that forwards packets between IP networks. For that, a router performs IP routing, which is the process of determining the next hop to forward a packet to based on the packet destination IP address. FortiGate supports both IPv4 and IPv6 routing.

FortiGate performs routing for both:

- ✓ firewall traffic (also known as user traffic)
- ✓ and local-out traffic.

Firewall traffic is the traffic that travels through FortiGate.
Local-out traffic is the traffic generated by FortiGate, usually for management purposes.

For example, when you ping a device from FortiGate, that's local-out traffic. When FortiGate connects to FortiGuard to download the latest definitions, that's also local-out traffic.



What Is IP Routing? (Contd)

- Routing table:
  - Contains routes with next-hop information for a destination
  - Entries are checked during route lookup (best route selection)
  - *Best route*: most specific route to the destination
  - *Duplicate routes*: multiple routes to the same destination
    - Route attributes are used as tiebreakers for best route selection
- Routing precedes most security actions
  - Configure your security policies based on routing settings, not the opposite

Routing Table?

Routers maintain a routing table. A routing table contains a series of entries, also known as routes.

Next Hop?

Each route in the routing table indicates the next hop for a particular destination. The next hop refers to the outgoing interface and gateway to use for forwarding the packet. The next hop can be the destination of the packet or another router along the path to the destination. If the next hop isn’t the destination, the next router in the path routes the packet to the next hop.

Routing Process?

The routing process is repeated on each router along the path until the packet reaches its destination.

Route Lookup?

To route packets, FortiGate performs a route lookup to identify the best route to the destination.

Best Route?

The best route is the most specific route to the destination.

Duplicate Routes?

If FortiGate finds duplicate routes—multiple routes to the same destination—it uses various route attributes as a tiebreaker to determine the best route.

Note That:

Routing takes place before most security features. For example, routing precedes firewall policy evaluation, content inspection, traffic shaping, and source NAT (SNAT). This means that the security actions that FortiGate performs depend on the outgoing interface determined by the routing process. This also means that your security policy configuration must follow your routing configuration, and not the opposite.

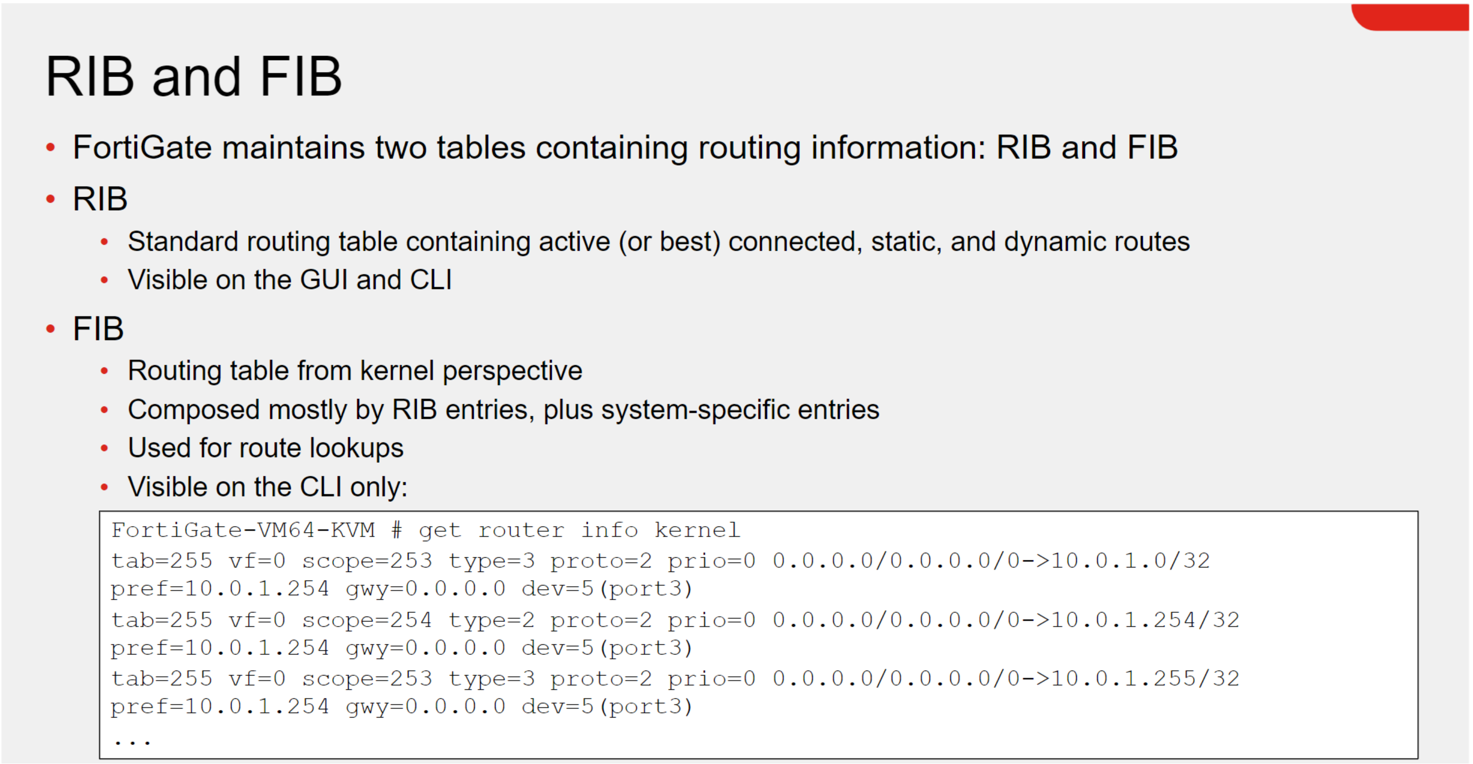
Route Lookup

For each session, FortiGate performs two route lookups:

- For the first packet sent by the originator
- For the first reply packet coming from the responder

After completing these two lookups, FortiGate writes the routing information to its **session table**. Subsequent packets are routed according to the session table, not the routing table. So, all packets that belong to the same session follow the same path. However, there is an exception to this rule: if there is a change in the routing table that impacts the session, then FortiGate removes the route information for the session table, and then performs additional route lookups to rebuild this information.

RIB and FIB



RIB and FIB

- FortiGate maintains two tables containing routing information: RIB and FIB
- RIB
  - Standard routing table containing active (or best) connected, static, and dynamic routes
  - Visible on the GUI and CLI
- FIB
  - Routing table from kernel perspective
  - Composed mostly by RIB entries, plus system-specific entries
  - Used for route lookups
  - Visible on the CLI only:

```
FortiGate-VM64-KVM # get router info kernel
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.0/32
pref=10.0.1.254 gwy=0.0.0.0 dev=5(port3)
tab=255 vf=0 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.254/32
pref=10.0.1.254 gwy=0.0.0.0 dev=5(port3)
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.255/32
pref=10.0.1.254 gwy=0.0.0.0 dev=5(port3)
...
```

FortiGate maintains its routing information in two tables:

✓ RIB:

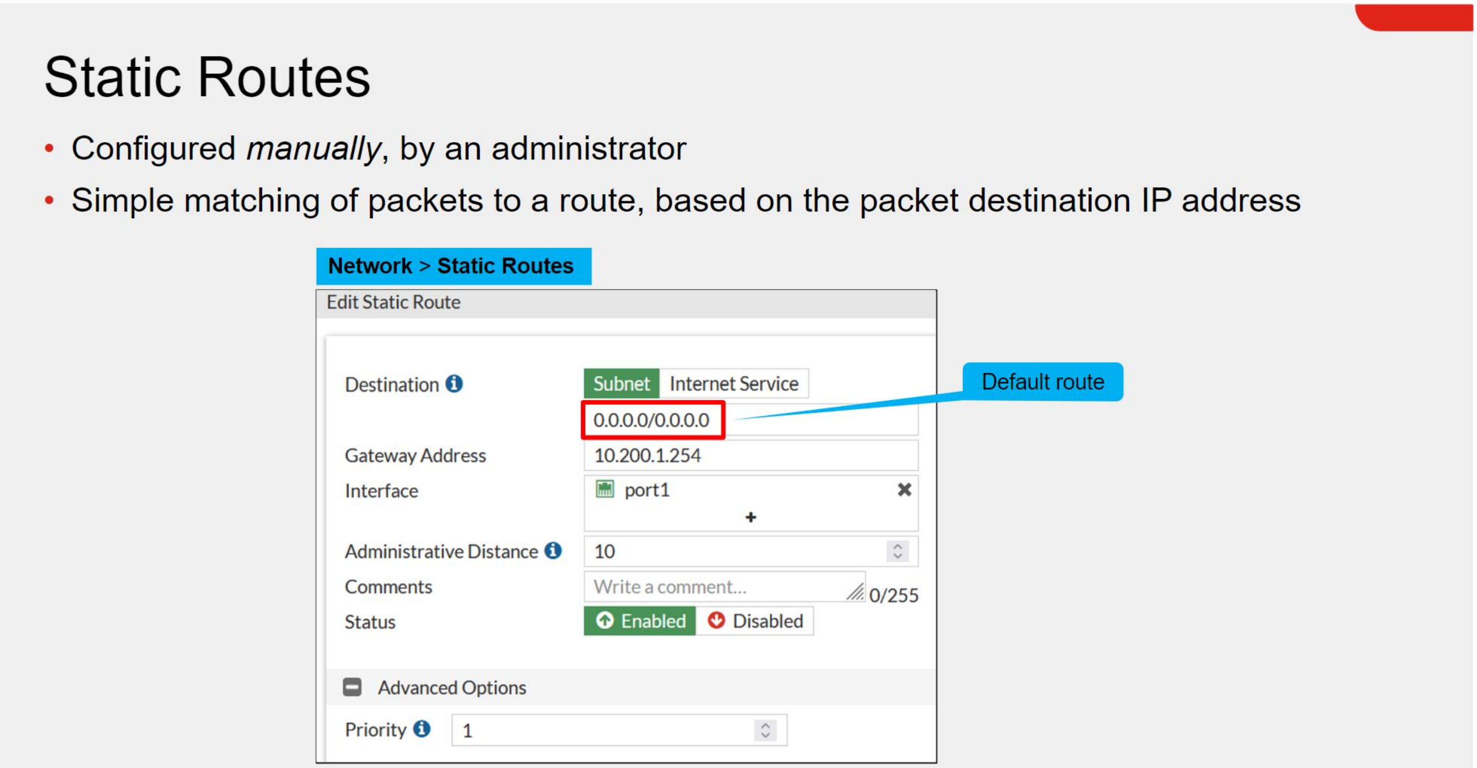
The routing table, also known as the routing information base (RIB), is a standard routing table containing active (or the best) connected, static, and dynamic routes.

✓ FIB:

The forwarding information base (FIB) can be described as the routing table from the kernel point of view, and is built mostly out of RIB entries plus some system-specific entries required by FortiOS.

When FortiGate performs a **route lookup**, **it checks the FIB and not the RIB**. However, because the FIB is composed mostly by RIB entries, then the route lookup mainly involves checking routes from the RIB. For this reason, the route lookup is often referred to as the routing table lookup process. Nonetheless, a more accurate statement is to refer to it as the FIB lookup process. You can display the **RIB entries** on the FortiGate **GUI and CLI**. However, **for the FIB**, you can display its entries on the FortiGate **CLI only**. The output on this slide shows the CLI command that displays the FIB.

Static Route



Static Routes

- Configured *manually*, by an administrator
- Simple matching of packets to a route, based on the packet destination IP address

Network > Static Routes

Edit Static Route

Destination: Subnet | Internet Service — 0.0.0.0/0.0.0.0

Gateway Address: 10.200.1.254

Interface: port1

Administrative Distance: 10

Comments: Write a comment... 0/255

Status: Enabled | Disabled

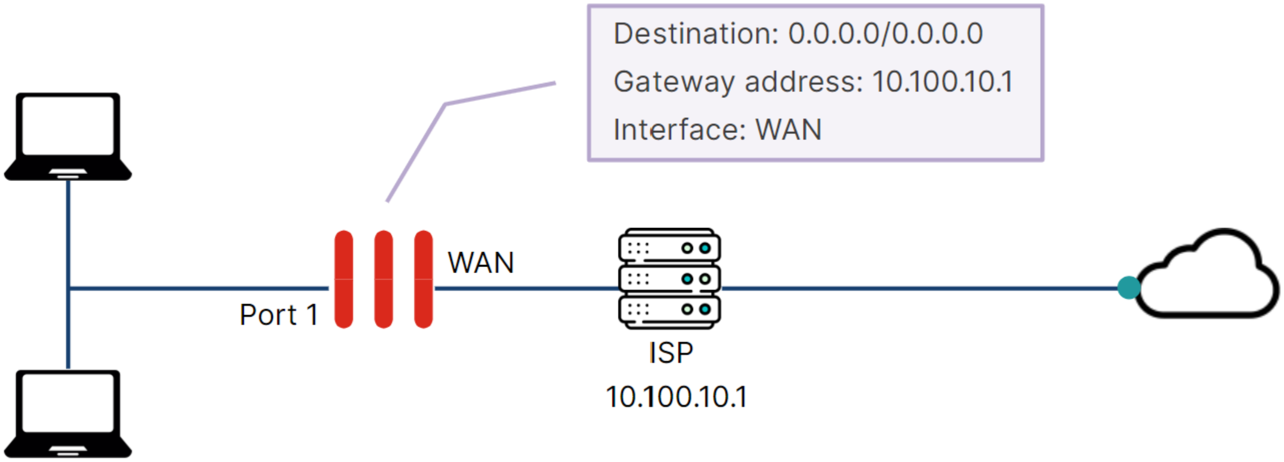
Advanced Options

Priority: 1

One type of manually configured route is called a **static route**. When you configure a static route, you are telling FortiGate, “When you see a packet whose destination is within a specific range, send it through a specific network interface, towards a specific router.”

You can also configure the **distance** and **priority** so that FortiGate can identify the best route to any destination matching multiple routes.

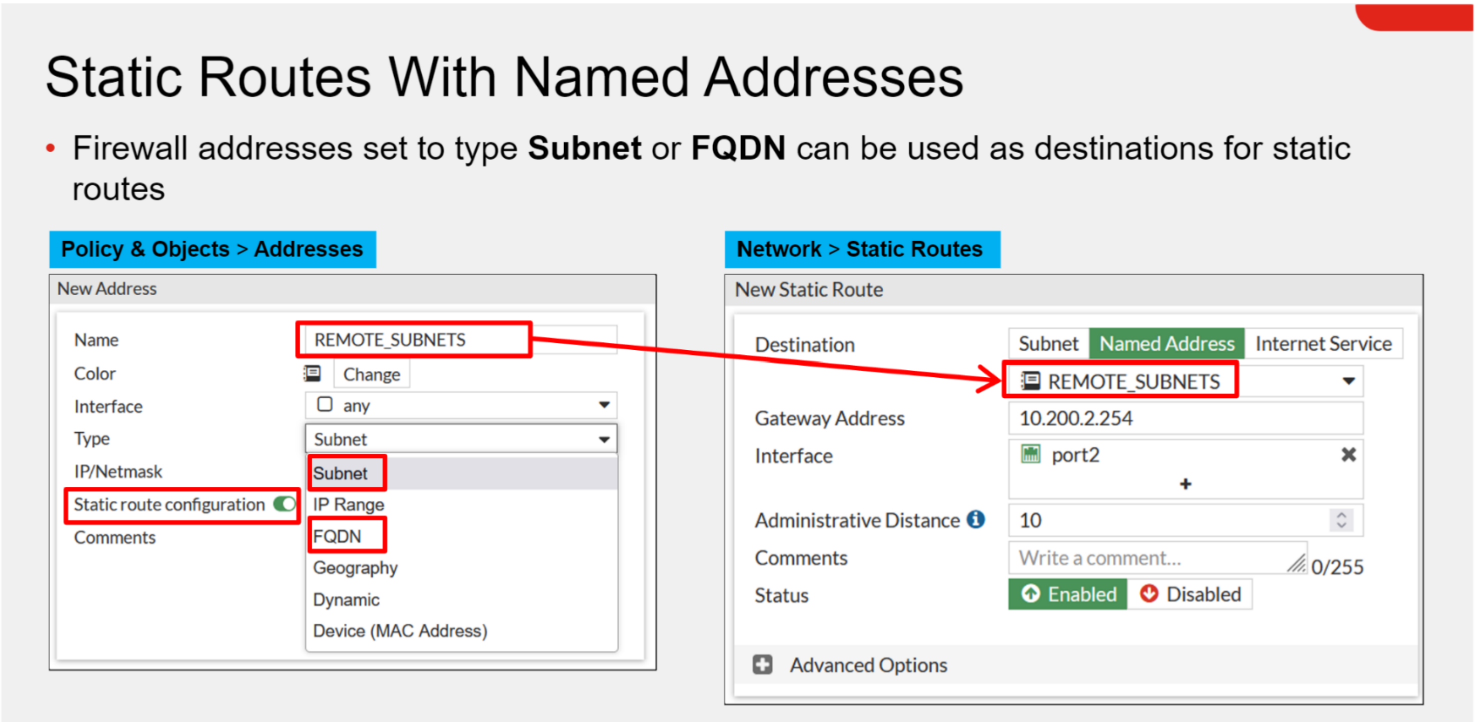
For example, in simple home networks, DHCP automatically retrieves and configures a route. Your modem then sends all outgoing traffic through your ISP internet router, which can relay packets to their destination. This is typically referred to as a **default route**, because all traffic not matching any other routes will, by default, be routed using this route. The example shown on this slide is a default route. The destination subnet value of 0.0.0.0/0.0.0.0 matches all addresses within any subnet. Most FortiGate devices deployed at the edge of the network have at least one of these default routes to ensure internet traffic is forwarded to the ISP network. Static routes are not needed for subnets to which FortiGate has direct Layer 2 connectivity.


Destination: 0.0.0.0/0.0.0.0
Gateway address: 10.100.10.1
Interface: WAN

The default route tells FortiGate where to send traffic when packets do not include an exact match for the destination address in the FortiGate routing table. Usually, all the users that are behind FortiGate need a default route in order to have internet access.

In the default route, the destination address is set to 0.0.0.0. The gateway address is typically the address of another router, either a device in your network that is between FortiGate and the network edge, or part of your ISP network if FortiGate is located on the network edge. Finally, the interface is the FortiGate port that connects to that router, typically the WAN interface.

Static Routes with Named Addresses



Static Routes With Named Addresses

- Firewall addresses set to type **Subnet** or **FQDN** can be used as destinations for static routes

Policy & Objects > Addresses

New Address

Name: REMOTE_SUBNETS

Color: Change

Interface: any

Type: Subnet

IP/Netmask

Static route configuration: enabled

Comments

Network > Static Routes

New Static Route

Destination: Subnet | Named Address | Internet Service — Named Address: REMOTE_SUBNETS

Gateway Address: 10.200.2.254

Interface: port2

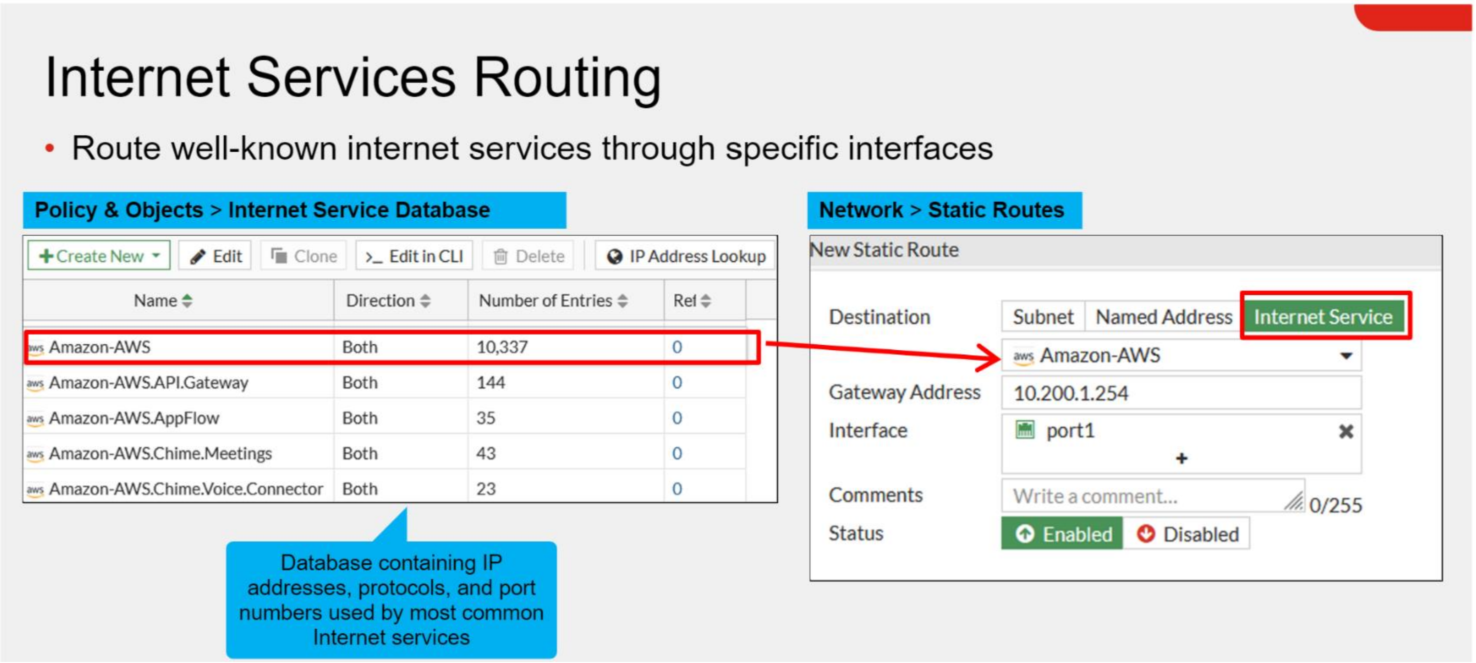
Administrative Distance: 10

Comments: Write a comment... 0/255

Status: Enabled | Disabled

If you create a firewall address object with the type **Subnet** or **FQDN**, you can use that firewall address as the destination of one or more static routes. First, enable **Static route configuration** in the firewall address configuration. After you enable it, the firewall address object becomes available for use in the **Destination** drop-down list for static routes with named addresses.

Internet Services Routing



Internet Services Routing

- Route well-known internet services through specific interfaces

Policy & Objects > Internet Service Database

Name	Direction	Number of Entries	Ref
Amazon-AWS	Both	10,337	0
Amazon-AWS.API.Gateway	Both	144	0
Amazon-AWS.AppFlow	Both	35	0
Amazon-AWS.Chime.Meetings	Both	43	0
Amazon-AWS.Chime.Voice.Connector	Both	23	0

Database containing IP addresses, protocols, and port numbers used by most common Internet services

Network > Static Routes

New Static Route

Destination: Subnet | Named Address | Internet Service — Internet Service: Amazon-AWS

Gateway Address: 10.200.1.254

Interface: port1

Comments: Write a comment... 0/255

Status: Enabled | Disabled

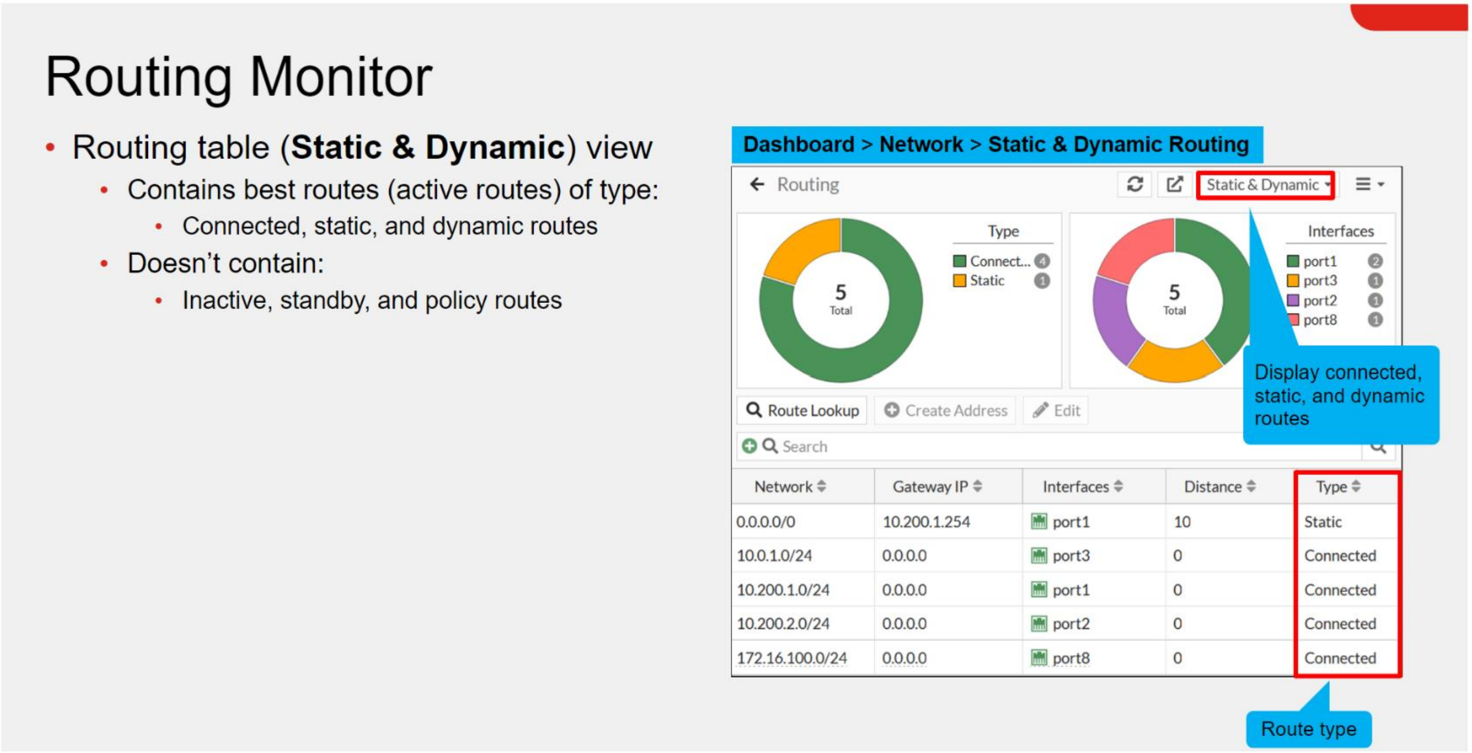
What happens if you need to route traffic to a public internet service (such as Amazon-AWS or Apple Store) through a specific WAN link? Say you have two ISPs and you want to route Netflix traffic through one ISP and all your other internet traffic though the other ISP. To achieve this goal:

You need to know the Netflix IP addresses and configure the static route. After that, you must frequently check that none of the IP addresses have changed.

But:

The internet service database (ISDB) helps make this type of routing easier and simpler. ISDB entries are applied to static routes to selectively route traffic though specific WAN interfaces. Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table.

Routing Monitor



Routing Monitor

- Routing table (**Static & Dynamic**) view
  - Contains best routes (active routes) of type:
    - Connected, static, and dynamic routes
  - Doesn't contain:
    - Inactive, standby, and policy routes

Dashboard > Network > Static & Dynamic Routing

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

Display connected, static, and dynamic routes

Route type

The routing monitor widget on the dashboard page enables you to view the **routing table** and **policy route table** entries. Dashboard > Network > Static & Dynamic Routing

The routing table contains the best routes (or active routes) of the following type:

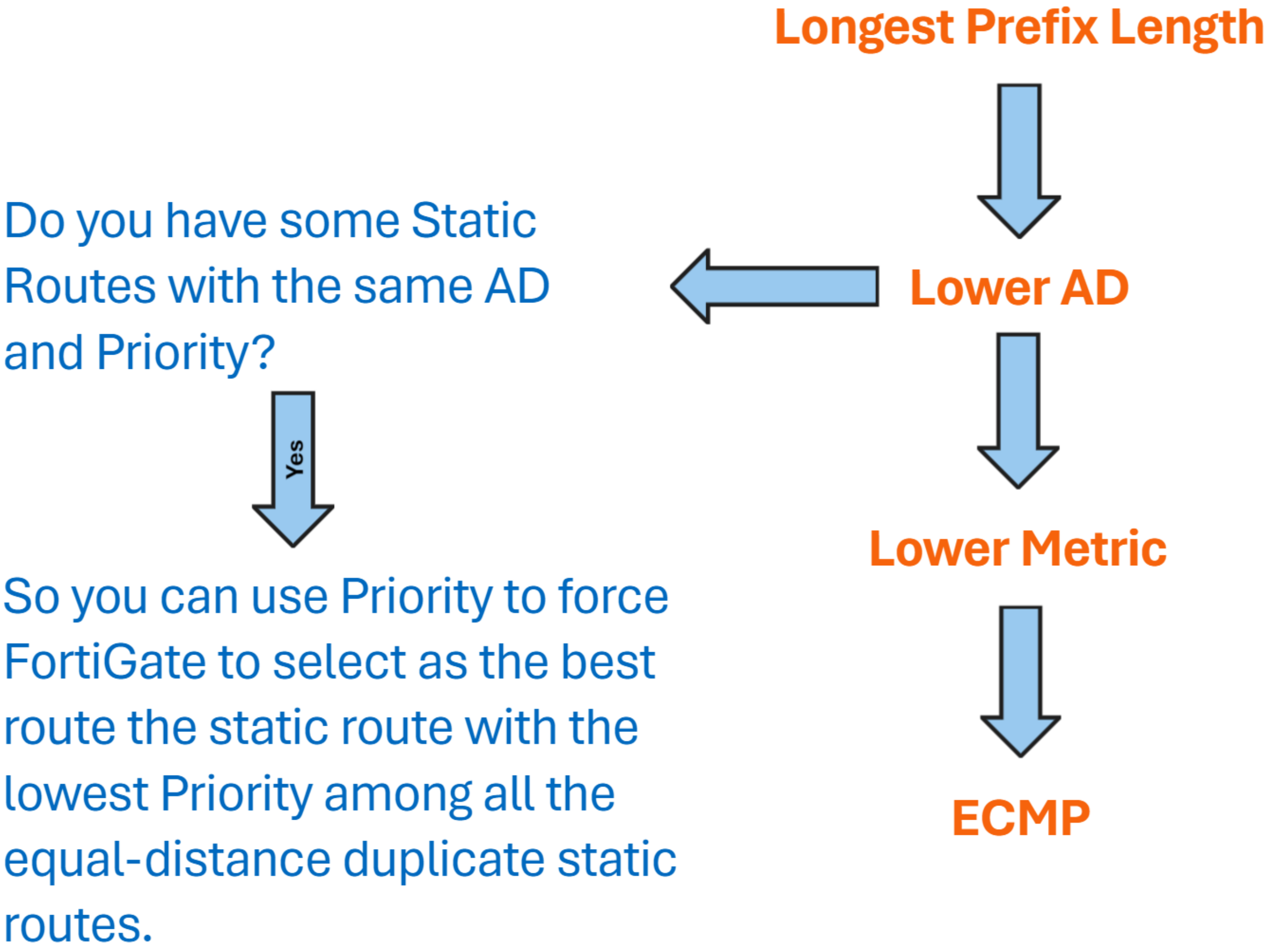
- **Static:** manual routes that are configured by the administrator.
- **Connected:** automatic routes added by FortiOS after an interface is assigned an IP address. A connected route references the interface IP address subnet.
- **Dynamic:** routes learned using a dynamic routing protocol such as BGP or OSPF. FortiGate installs these routes automatically in the routing table and indicates the dynamic routing protocol used.

To view the routing table entries, select **Static & Dynamic**, as shown on this slide. However, keep in mind that the routing table doesn't contain the following routes:

- **Inactive routes:** static and connected routes whose interfaces are administratively down or whose links are down. Static routes are also marked inactive when their gateway is detected as dead by the link health monitor.
- **Standby routes:** These are active routes that are removed from the routing table because they are duplicate and have higher distances. For instance:
  - ➢ A second static default route with a higher distance than another static default route.
  - ➢ A dynamic route such as BGP or OSPF, to the same destination as another static route. However, the dynamic route is not displayed in the routing table because the static route has a lower distance.

- **Policy routes:** These include **regular policy routes (PBR)**, **ISDB routes**, and **SD-WAN rules**. Policy routes are viewed in a separate table— the policy route table. To view the policy route table entries, select **Policy**.

Best Route Selection



Longest Prefix Length

Lower AD

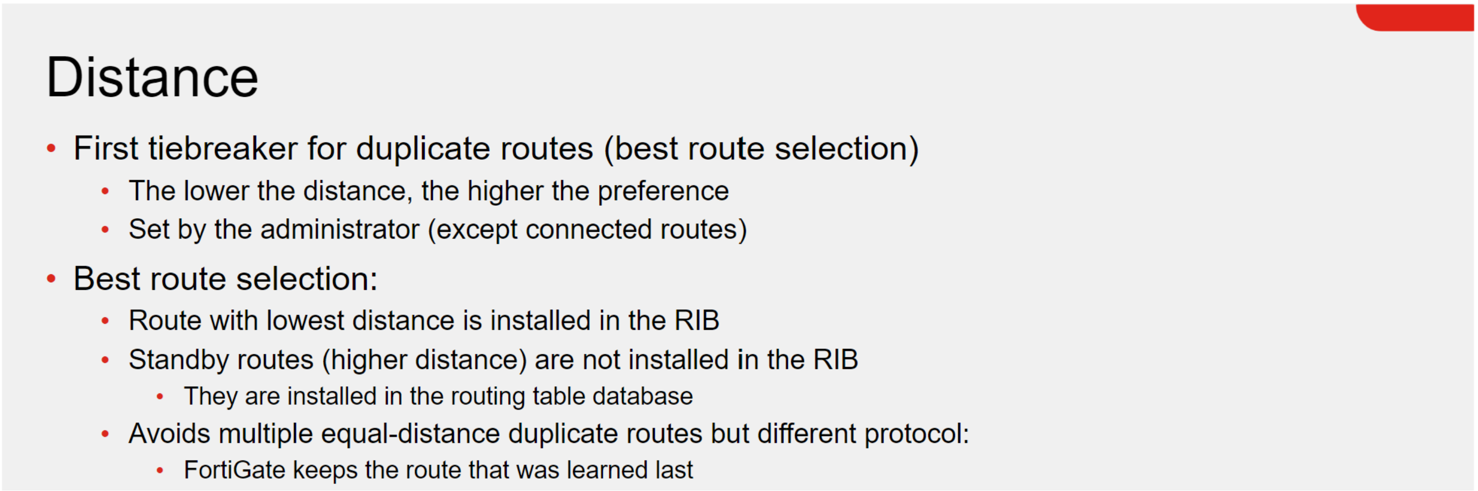
Lower Metric

ECMP

Do you have some Static Routes with the same AD and Priority?

So you can use Priority to force FortiGate to select as the best route the static route with the lowest Priority among all the equal-distance duplicate static routes.

Administrative Distance



Distance

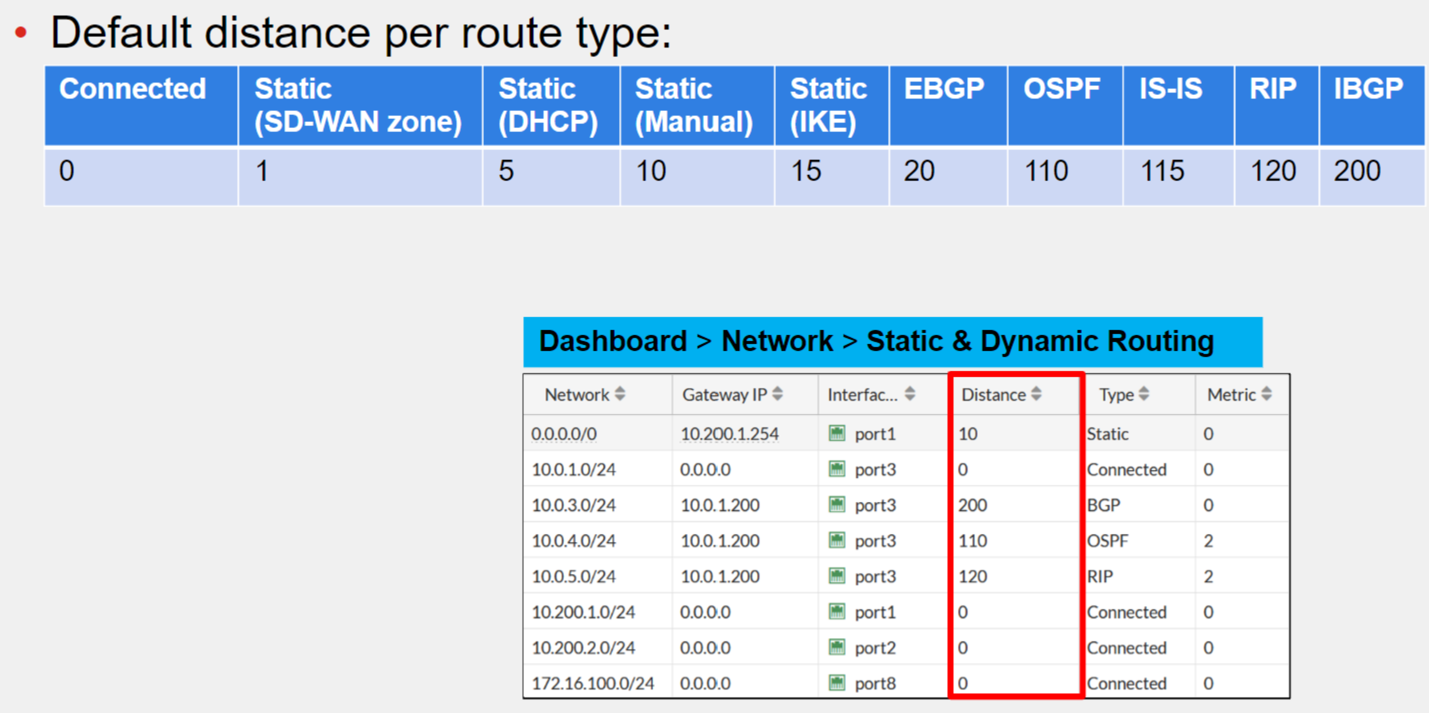
- First tiebreaker for duplicate routes (best route selection)
  - The lower the distance, the higher the preference
  - Set by the administrator (except connected routes)
- Best route selection:
  - Route with lowest distance is installed in the RIB
  - Standby routes (higher distance) are not installed in the RIB
    - They are installed in the routing table database
  - Avoids multiple equal-distance duplicate routes but different protocol:
    - FortiGate keeps the route that was learned last

Distance, or administrative distance (AD), is the first tiebreaker that routers use to determine the best route for a particular destination. If there are two or more routes to the same destination (duplicate routes), the lowest-distance route is considered the best route and, as a result, is installed in the routing table. Other lower-distance routes to the same destination are standby routes and, as a result, are not installed in the routing table. Instead, **they are installed in the routing table database**.

Lower AD Route ➔ is Installed in the Routing Table

Other lower-distance routes ➔ are Installed in the Routing Table Database

Default Administrative Distance:



- Default distance per route type:

Connected	Static (SD-WAN zone)	Static (DHCP)	Static (Manual)	Static (IKE)	EBGP	OSPF	IS-IS	RIP	IBGP
0	1	5	10	15	20	110	115	120	200

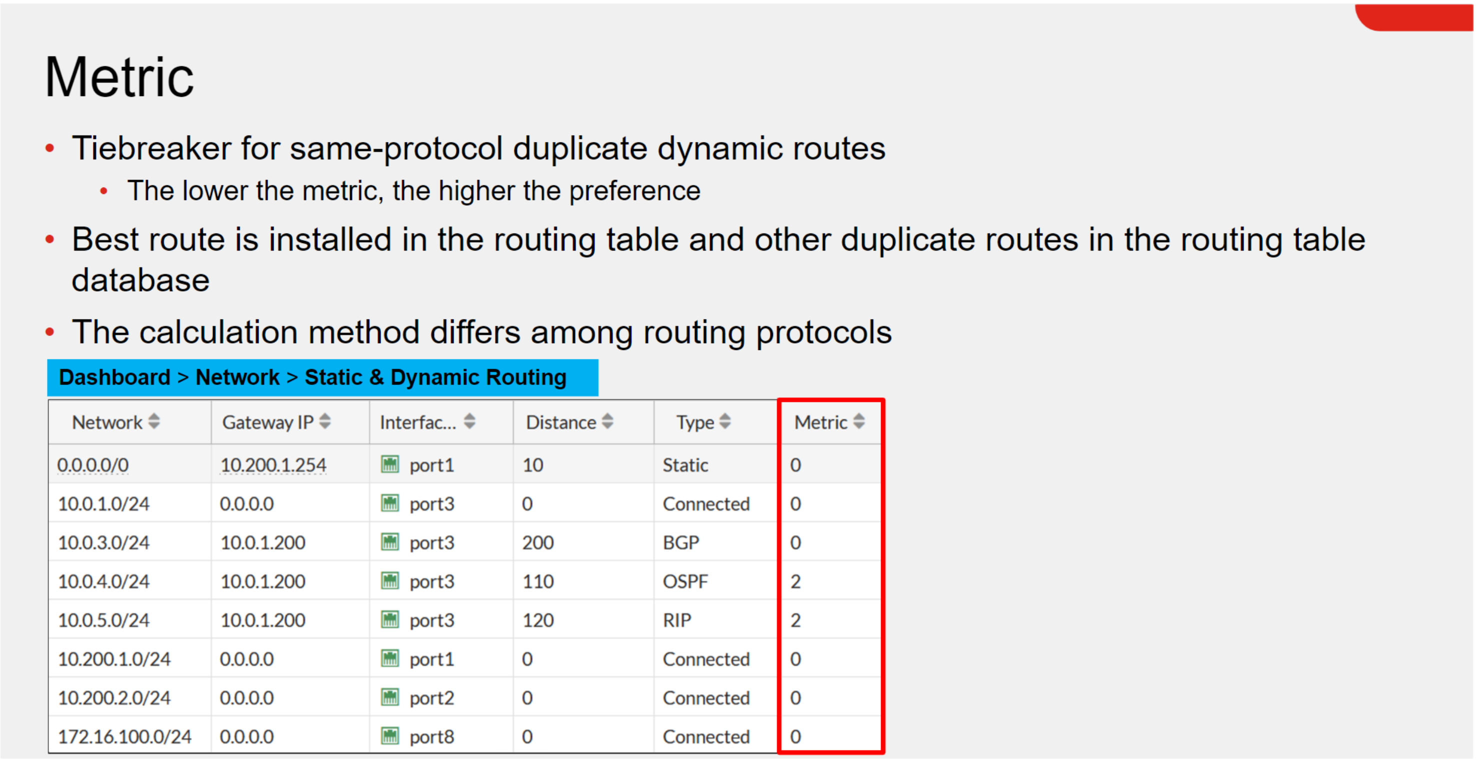
Dashboard > Network > Static & Dynamic Routing

Network	Gateway IP	Interfac...	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
10.0.3.0/24	10.0.1.200	port3	200	BGP	0
10.0.4.0/24	10.0.1.200	port3	110	OSPF	2
10.0.5.0/24	10.0.1.200	port3	120	RIP	2
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

You can set the distance for all route types **except connected and IS-IS routes**—both are hardcoded and their distance value cannot change.

In case FortiGate learns two equal-distance routes to the same destination but that are sourced from different protocols, then **FortiGate installs in the routing table the route that was learned last**. For example, if you set the distance of BGP routes to 110, and there is another OSPF route to the same destination using the default administrative distance (110), then FortiGate keeps whichever route was learned last in the routing table. Because this behavior can lead to different results based on the timing of events, then it’s not recommended to configure differentprotocol routes with the same distance.

Metric



Metric

- Tiebreaker for same-protocol duplicate dynamic routes
  - The lower the metric, the higher the preference
- Best route is installed in the routing table and other duplicate routes in the routing table database
- The calculation method differs among routing protocols

Dashboard > Network > Static & Dynamic Routing

Network	Gateway IP	Interfac...	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
10.0.3.0/24	10.0.1.200	port3	200	BGP	0
10.0.4.0/24	10.0.1.200	port3	110	OSPF	2
10.0.5.0/24	10.0.1.200	port3	120	RIP	2
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

When a dynamic route protocol learns two or more routes to the same destination, it uses the **metric as a tiebreaker** to identify the best route. The lower the metric, the higher the preference. **The dynamic routing protocol then installs the best route in the routing table** and **the higher metric routes in the routing table database**.

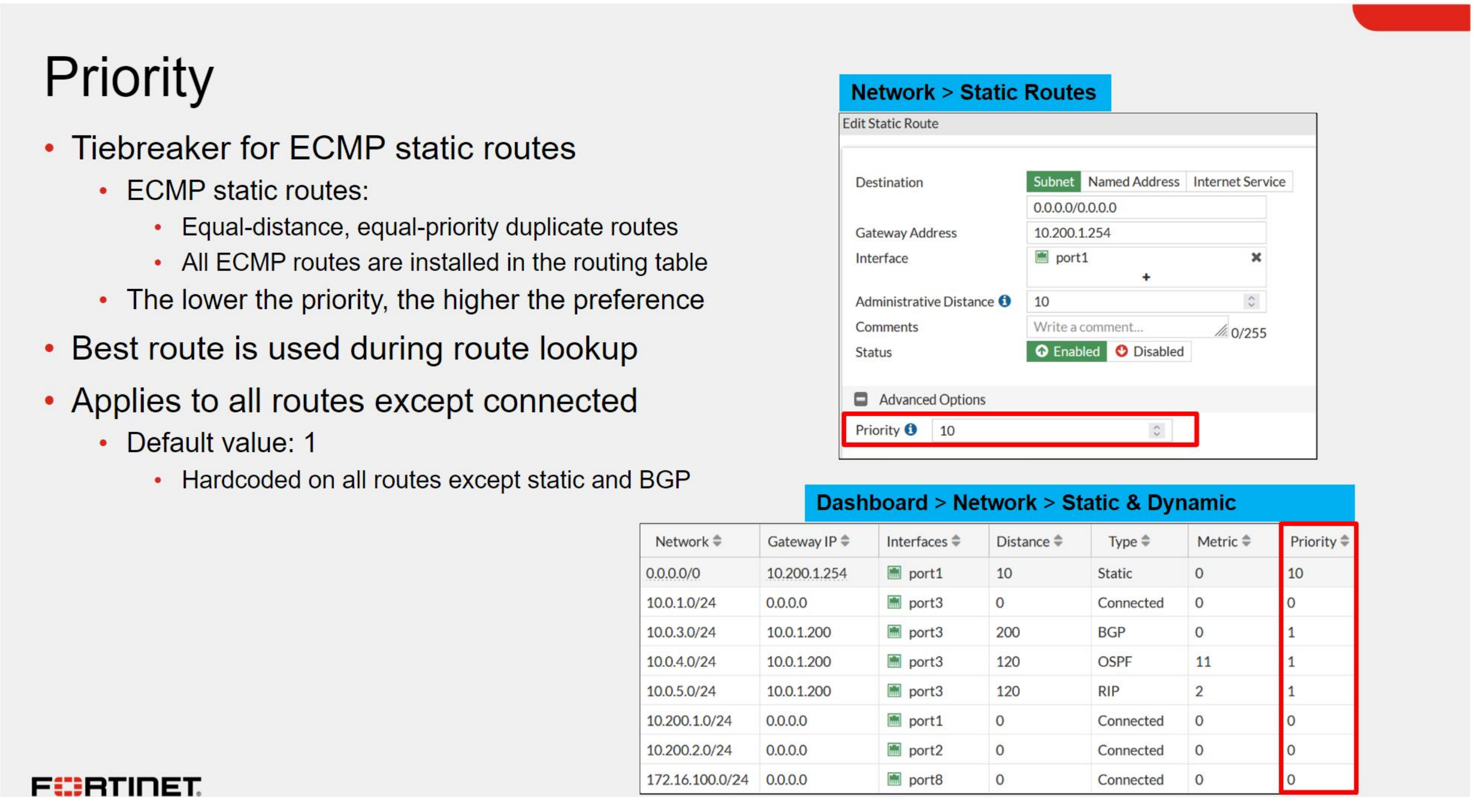
Lower Metric Route ➔ is Installed in the Routing Table

Higher Metric routes ➔ are Installed in the Routing Table Database

Note that the metric is used as tiebreaker for **same protocol dynamic routes**, and not between different-protocol dynamic routes.

The metric calculation differs among routing protocols. For example, RIP uses the hop count, which is the number of routers the packet must pass through to reach the destination. OSPF uses cost, which is determined by the link bandwidth.

Priority



Priority

- Tiebreaker for ECMP static routes
  - ECMP static routes:
    - Equal-distance, equal-priority duplicate routes
    - All ECMP routes are installed in the routing table
  - The lower the priority, the higher the preference
- Best route is used during route lookup
- Applies to all routes except connected
  - Default value: 1
    - Hardcoded on all routes except static and BGP

Network > Static Routes

Edit Static Route

Destination	Subnet · Named Address · Internet Service 0.0.0.0/0.0.0.0
Gateway Address	10.200.1.254
Interface	port1
Administrative Distance	10
Comments	Write a comment... 0/255
Status	Enabled · Disabled

Advanced Options

Priority	10

Dashboard > Network > Static & Dynamic

Network	Gateway IP	Interfaces	Distance	Type	Metric	Priority
0.0.0.0/0	10.200.1.254	port1	10	Static	0	10
10.0.1.0/24	0.0.0.0	port3	0	Connected	0	0
10.0.3.0/24	10.0.1.200	port3	200	BGP	0	1
10.0.4.0/24	10.0.1.200	port3	120	OSPF	11	1
10.0.5.0/24	10.0.1.200	port3	120	RIP	2	1
10.200.1.0/24	0.0.0.0	port1	0	Connected	0	0
10.200.2.0/24	0.0.0.0	port2	0	Connected	0	0
172.16.100.0/24	0.0.0.0	port8	0	Connected	0	0

What is ECMP static routes?

When there are two or more duplicate static routes that have the same distance, FortiGate installs all of them in the routing table. **If they also have the same priority, then the routes are known as ECMP static routes**, and you will learn more about them in this lesson.

What is the Priority?

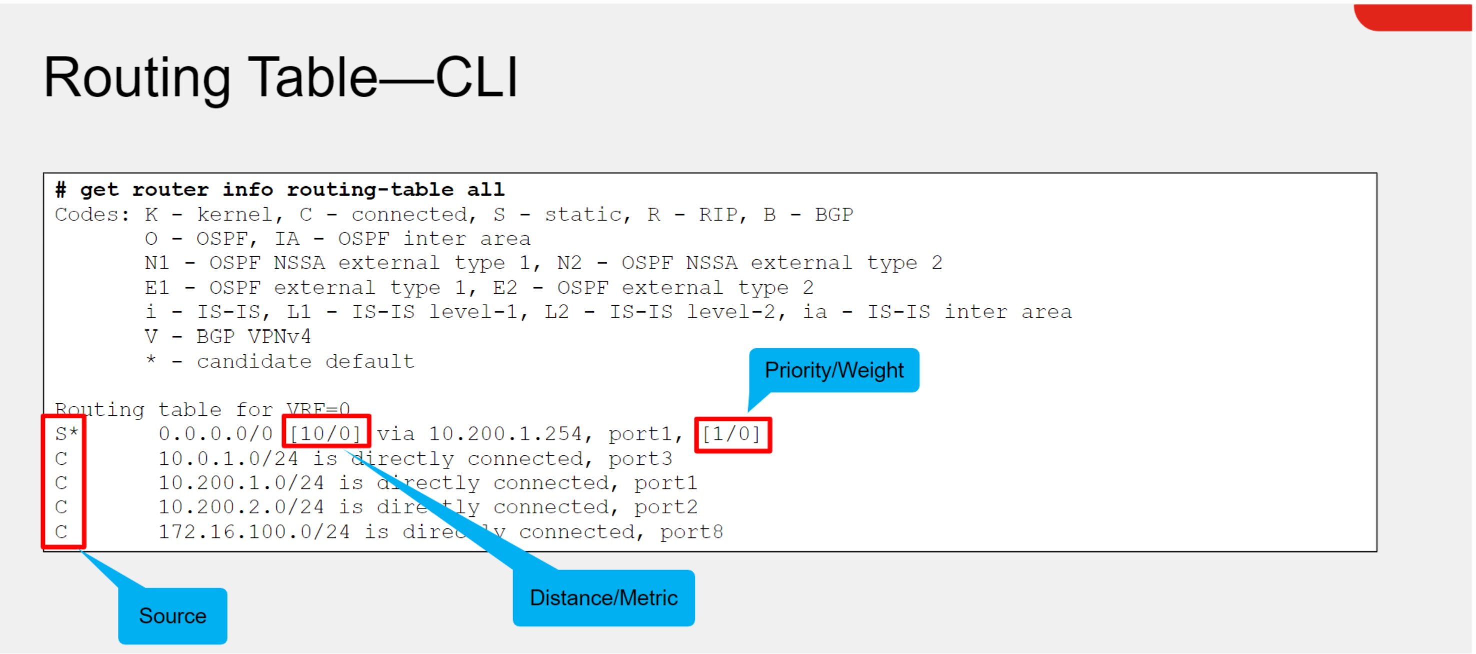
The priority setting enables administrators to break the tie among ECMP static routes. The result is that, during the route lookup process, FortiGate selects as the best route the static route with the lowest priority among all the equal-distance duplicate static routes. The lower the priority value, the higher the preference.

The priority attribute applies to **all routes except connected routes** and is set to **1** by default. For dynamic routes, you can change the priority of **BGP routes only**. The priority of other dynamic routes is hardcoded to **1**.

The Priority use case?

The use of the priority value in dynamic routes is useful for advanced routing deployments involving SD-WAN and multiple virtual routing and forwarding (VRF) IDs. For static routes, you can configure the priority setting under the Advanced Options on the FortiGate GUI, as shown on this slide. To view the priority in the routing monitor widget, you must enable the priority column (disabled by default). You can also view the priority on the routing table on the FortiGate CLI.

Routing Table - CLI



Routing Table—CLI

```
# get router info routing-table all
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
       * - candidate default

Routing table for VRF=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
```

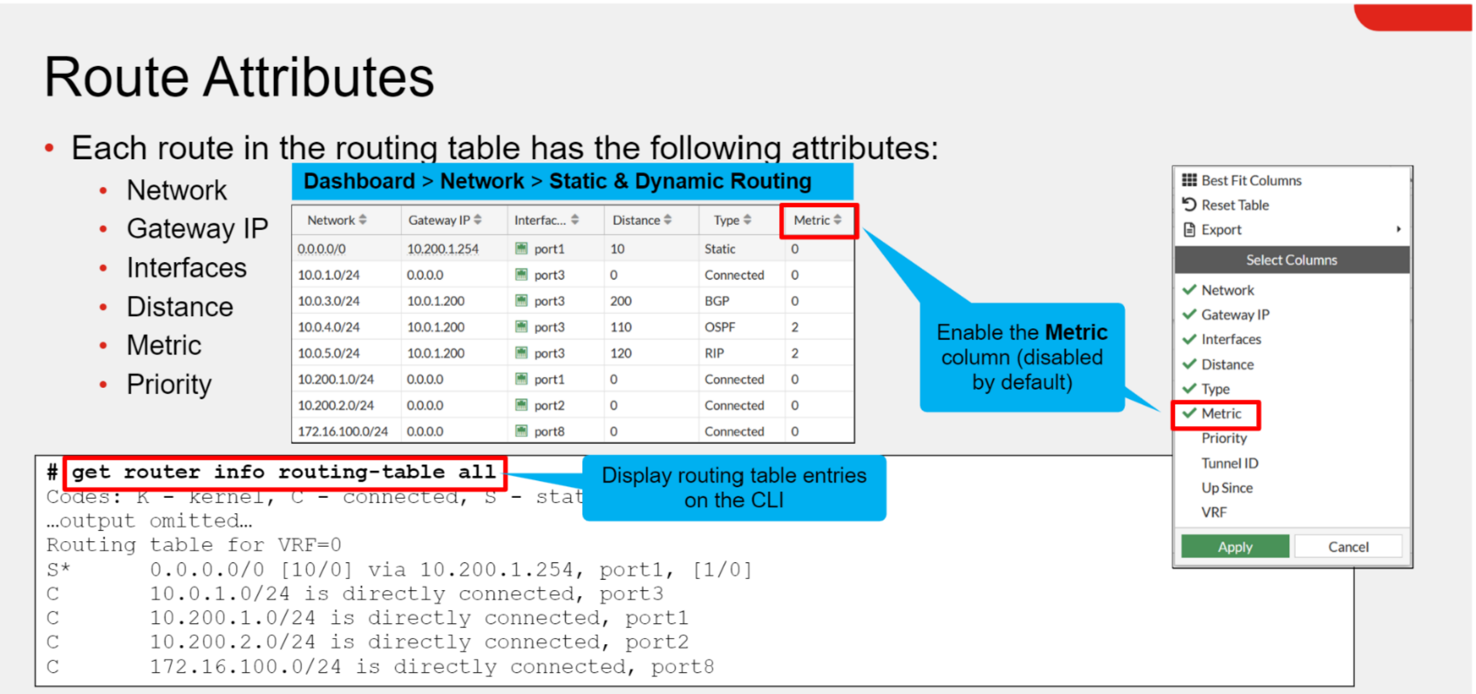
The CLI command shown on this slide displays all entries in the routing table. The routing table displays the routes that make it the best active routes to a destination. The left-most column indicates the route source. Route attributes are shown inside square brackets. The first number, in the first pair of attributes, is distance, which applies to both dynamic and static routes. The second number is metric, which applies to dynamic routes only. **Static routes** and **dynamic routes** also have **priority** and **weight attributes**, which are shown as the last pair of attributes for the respective route. **In the case of dynamic routes, the weight is always zero**.

Route Attributes?

AD, Metric, Priority, Weight, ...

This command doesn't show standby or inactive routes, which are present in the routing table database only. For example, when two static routes to the same destination subnet have different distances, the one with the lower distance is installed in the routing table, and the one with the higher distance in the routing table database.

Route Attributes



Route Attributes

- Each route in the routing table has the following attributes:
  - Network
  - Gateway IP
  - Interfaces
  - Distance
  - Metric
  - Priority

Dashboard > Network > Static & Dynamic Routing

Network	Gateway IP	Interfac...	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
10.0.3.0/24	10.0.1.200	port3	200	BGP	0
10.0.4.0/24	10.0.1.200	port3	110	OSPF	2
10.0.5.0/24	10.0.1.200	port3	120	RIP	2
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

Enable the **Metric** column (disabled by default)

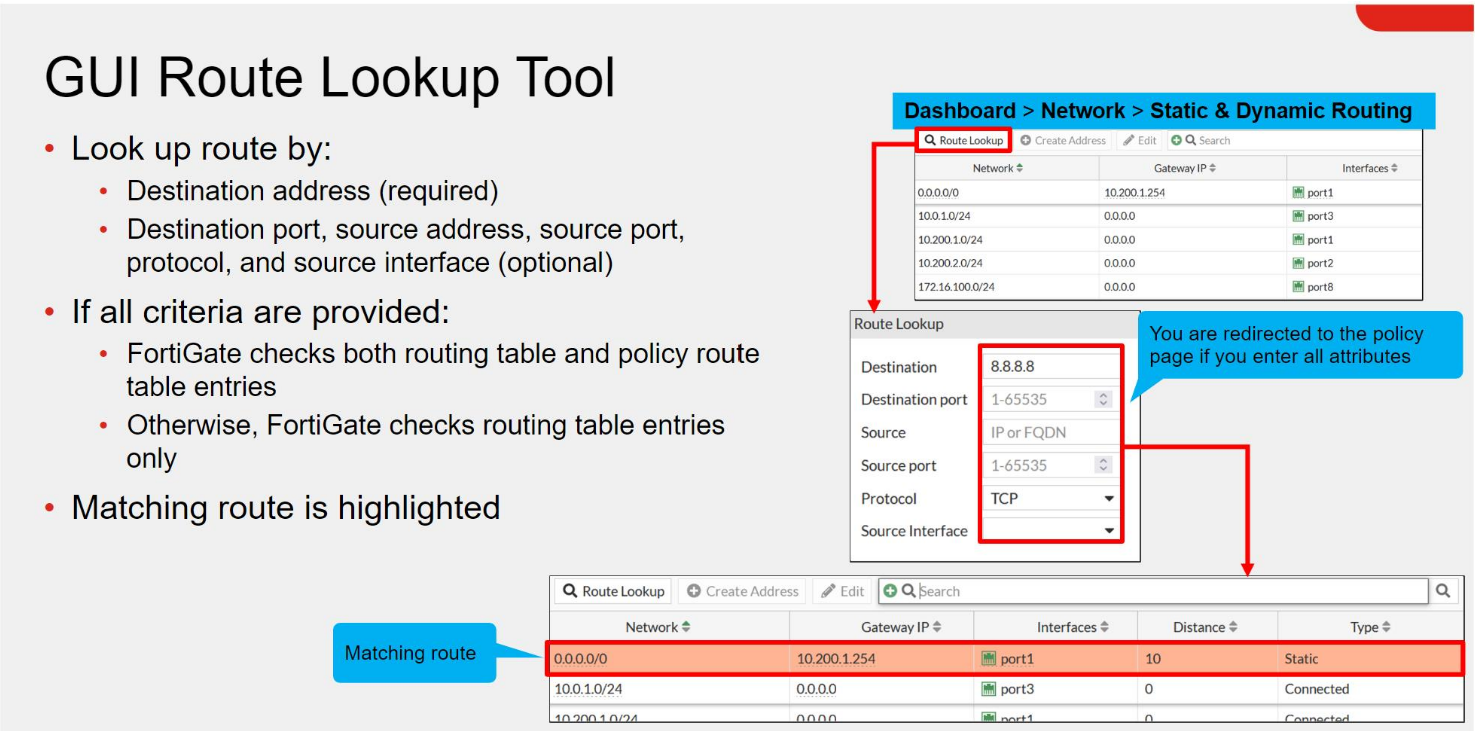
```
# get router info routing-table all
Codes: K - kernel, C - connected, S - stat
…output omitted…
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C       10.0.1.0/24 is directly connected, port3
C       10.200.1.0/24 is directly connected, port1
C       10.200.2.0/24 is directly connected, port2
C       172.16.100.0/24 is directly connected, port8
```

Display routing table entries on the CLI

Each of the routes listed in the routing table includes several attributes with associated values. The **Network** column lists the destination IP address and subnet mask to match. The **Interfaces** column lists the interface to use to deliver the packet. The **Distance**, **Metric**, and **Priority** attributes are used by FortiGate to make various route selection decisions.

This slide shows the command you can run to display the routing table on the FortiGate CLI. The `get router info routing-table all` command displays the same route entries as the routing monitor widget on the FortiGate GUI.

GUI Route Lookup Tool



GUI Route Lookup Tool

- Look up route by:
  - Destination address (required)
  - Destination port, source address, source port, protocol, and source interface (optional)
- If all criteria are provided:
  - FortiGate checks both routing table and policy route table entries
  - Otherwise, FortiGate checks routing table entries only
- Matching route is highlighted

Dashboard > Network > Static & Dynamic Routing

Network	Gateway IP	Interfaces
0.0.0.0/0	10.200.1.254	port1
10.0.1.0/24	0.0.0.0	port3
10.200.1.0/24	0.0.0.0	port1
10.200.2.0/24	0.0.0.0	port2
172.16.100.0/24	0.0.0.0	port8

Route Lookup

Destination	8.8.8.8
Destination port	1-65535
Source	IP or FQDN
Source port	1-65535
Protocol	TCP
Source Interface	

You are redirected to the policy page if you enter all attributes

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.200.1.254	port1	10	Static
10.0.1.0/24	0.0.0.0	port3	0	Connected
10.200.1.0/24	0.0.0.0	port1	0	Connected

Matching route

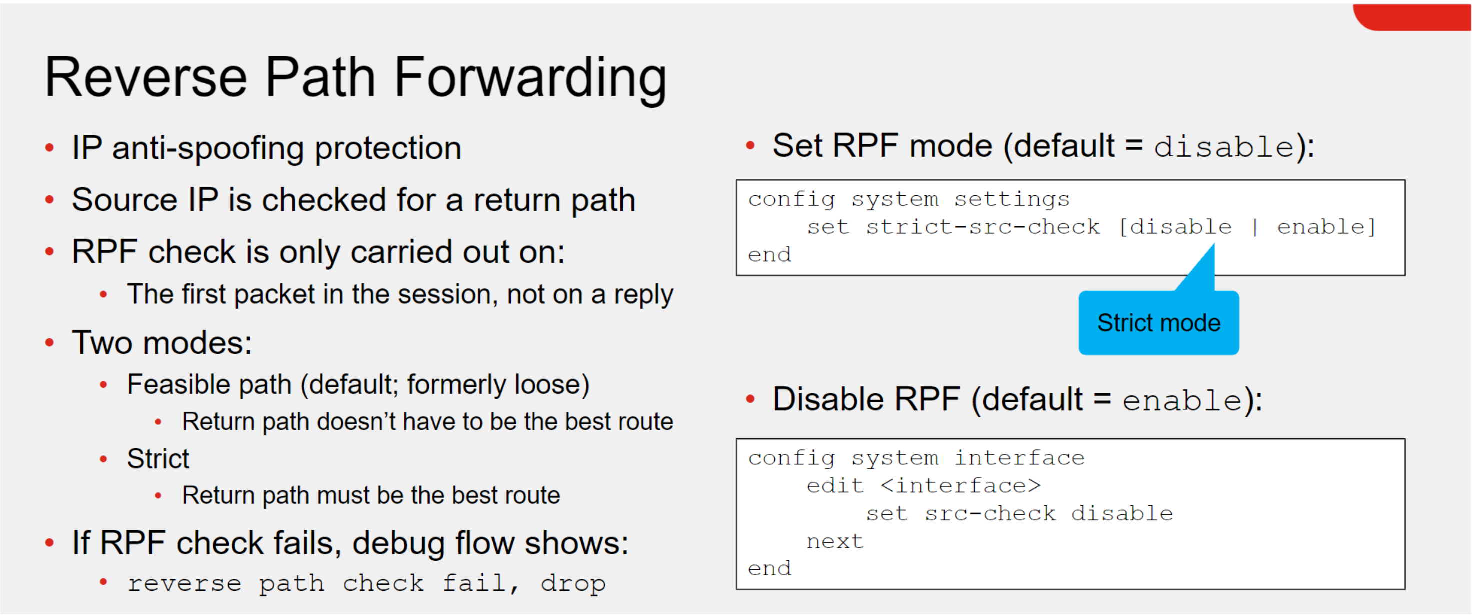
You can perform a route lookup on the routing monitor widget by clicking **Route Lookup**. Then, you must indicate at least the **destination address** to look up for, and optionally, the destination port, source address, source port, protocol, and source interface. The way the route lookup works is as follows:

- **If you don't provide all lookup criteria**, FortiGate considers **only the routing table entries**. FortiGate then highlights the matching route, if any.

- **If you provide all lookup criteria**, **FortiGate considers both routing table and policy table entries**.

If the lookup matches a policy route (PBR), the GUI redirects you to the policy route page, and then highlights the corresponding matching policy route. The example on this slide shows a route lookup tool for 8.8.8.8 and TCP as destination address and protocol, respectively. Because the administrator doesn't provide all criteria, FortiGate considers the routing table entries only. Then, the route lookup highlights the static default route as the matching route.

Reverse Path Forwarding (RPF)



Reverse Path Forwarding

- IP anti-spoofing protection
- Source IP is checked for a return path
- RPF check is only carried out on:
  - The first packet in the session, not on a reply
- Two modes:
  - Feasible path (default; formerly loose)
    - Return path doesn't have to be the best route
  - Strict
    - Return path must be the best route
- If RPF check fails, debug flow shows:
  - `reverse path check fail, drop`

- Set RPF mode (default = `disable`):

```
config system settings
    set strict-src-check [disable | enable]
end
```

Strict mode

- Disable RPF (default = `enable`):

```
config system interface
    edit <interface>
        set src-check disable
    next
end
```

The RPF check is a mechanism that protects FortiGate and your network from IP spoofing attacks by checking for a return path to the source in the routing table.

Whenever a packet arrives at one of the interfaces on a FortiGate, the FortiGate determines whether the packet was received on a legitimate interface by doing a reverse look-up using the source IP address in the packet header. This protects against IP spoofing attacks. If the FortiGate does not have a route to the source IP address through the interface on which the packet was received, the FortiGate **drops** the packet as per Reverse Path Forwarding (RPF) check.

The Process of the RPF Checking:

FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn't perform any additional RPF checks on that session.

There are two RPF check modes:

- **Feasible path:** Formerly known as loose, it’s the default mode. In this mode, FortiGate verifies that the routing table contains a route that matches the source address of the packet and the incoming interface. The matching route doesn’t have to be the best route in the routing table for that source address. It just has to match the source address and the incoming interface of the packet.

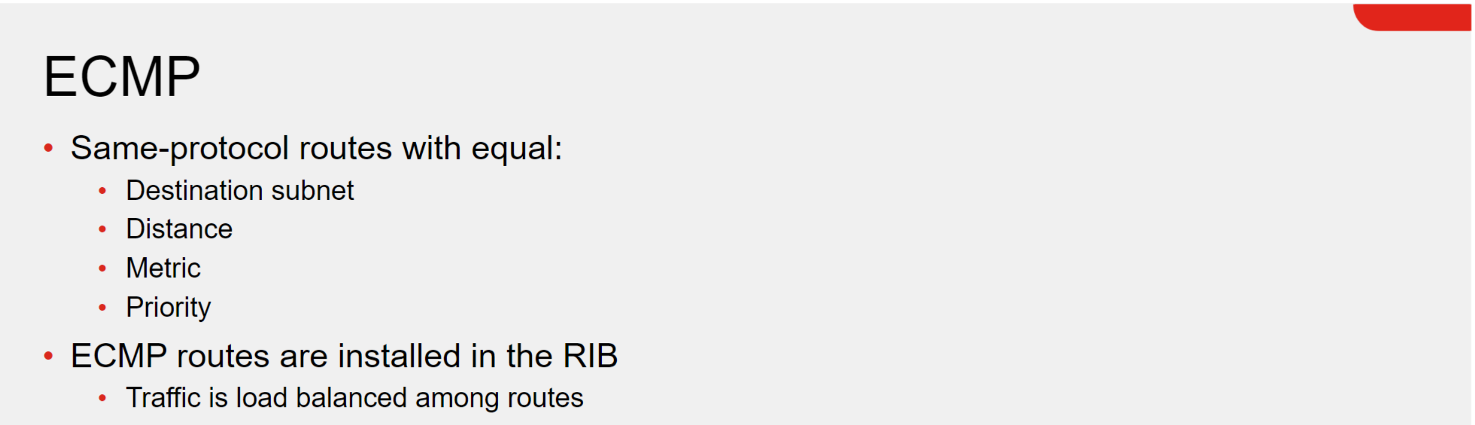
- **Strict:** In this mode, FortiGate also verifies that the matching route is the best route in the routing table. That is, if the routing table contains a matching route for the source address and incoming interface, but there is a better route for the source address through another interface, then, the RPF check fails.

This slide also shows how to change the RPF check mode on the FortiGate CLI, as well as how to disable the RPF check on the interface level.

If RPF check fails, debug flow shows:

```
Reverse path check fail, drop
```

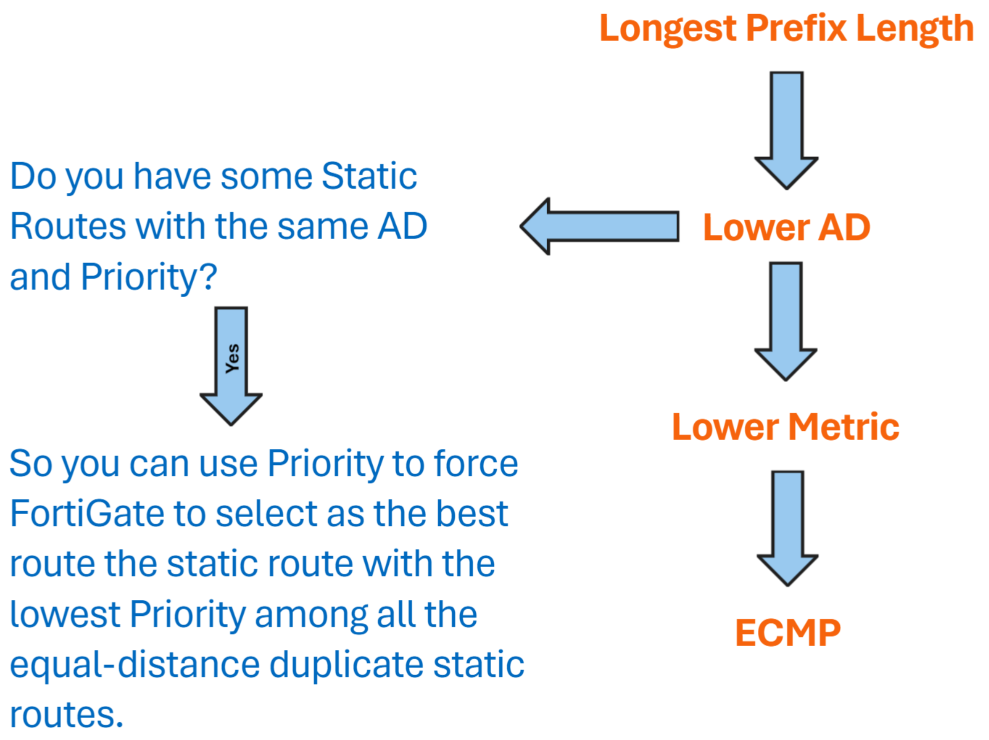
ECMP



ECMP

- Same-protocol routes with equal:
  - Destination subnet
  - Distance
  - Metric
  - Priority
- ECMP routes are installed in the RIB
  - Traffic is load balanced among routes

So far, you’ve learned about the different route attributes that FortiGate looks at to identify the best route to a destination. **But what happens when two or more routes of the same type have the same destination, distance, metric, and priority?** These routes are called equal cost multipath (ECMP) routes, and FortiGate installs all of them in the routing table. FortiGate also load balances the traffic among the ECMP routes.



Longest Prefix Length

Lower AD

Lower Metric

ECMP

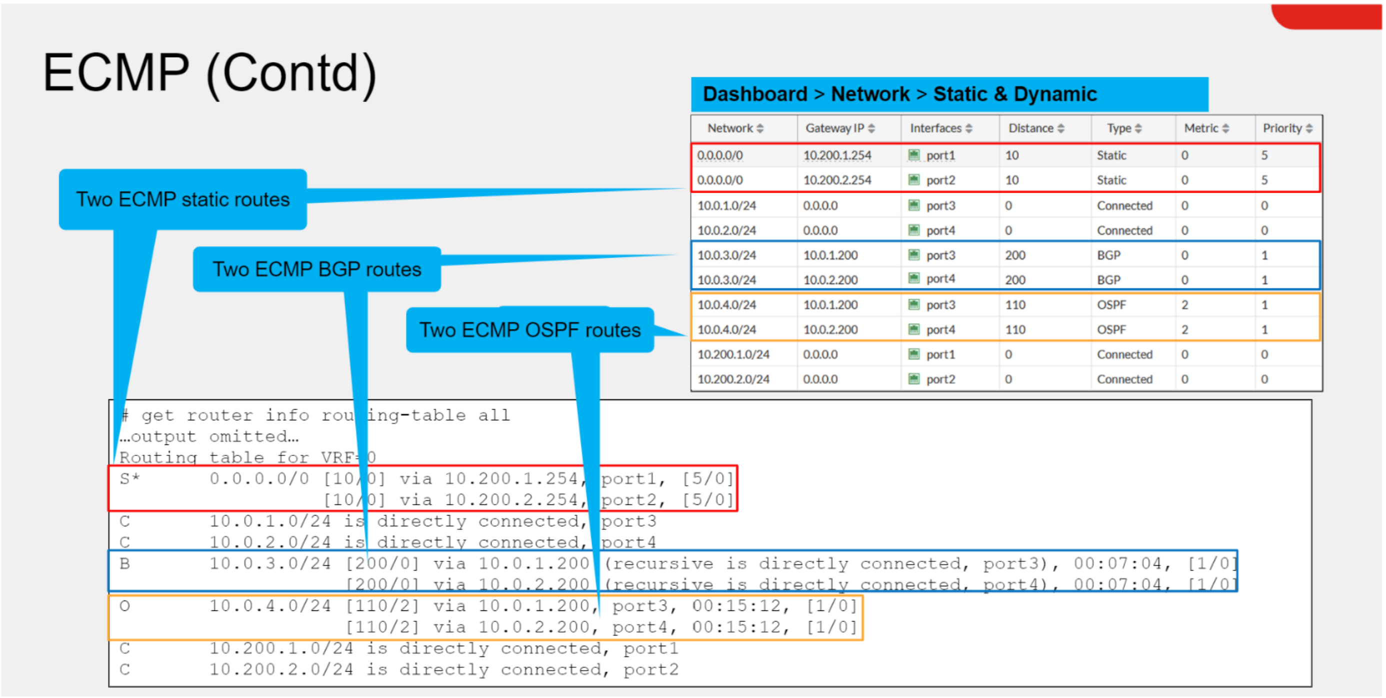
Do you have some Static Routes with the same AD and Priority?

So you can use Priority to force FortiGate to select as the best route the static route with the lowest Priority among all the equal-distance duplicate static routes.

ECMP pre-requisites are as follows:

- Routes must have the same destination and costs. In the case of static routes, costs include distance and priority
- Routes are sourced from the same routing protocol. Supported protocols include static routing, OSPF, and BGP

Example:



ECMP (Contd)

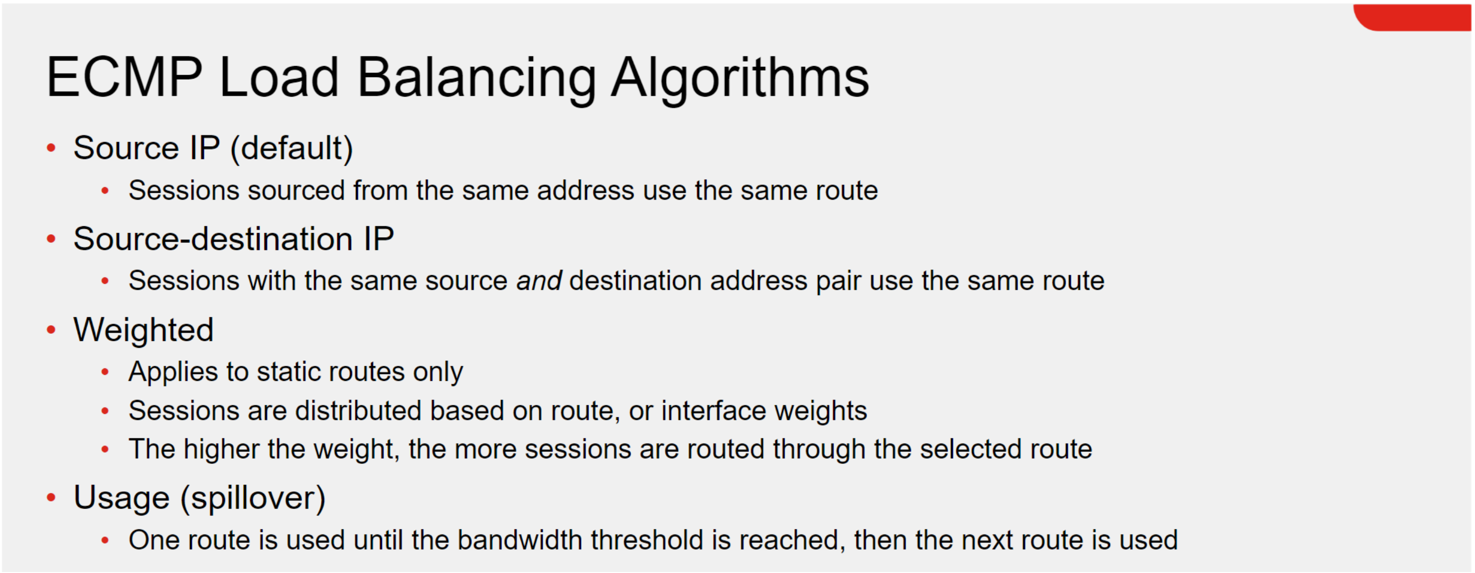
Dashboard > Network > Static & Dynamic

Network	Gateway IP	Interfaces	Distance	Type	Metric	Priority
0.0.0.0/0	10.200.1.254	port1	10	Static	0	5
0.0.0.0/0	10.200.2.254	port2	10	Static	0	5
10.0.1.0/24	0.0.0.0	port3	0	Connected	0	0
10.0.2.0/24	0.0.0.0	port4	0	Connected	0	0
10.0.3.0/24	10.0.1.200	port3	200	BGP	0	1
10.0.3.0/24	10.0.2.200	port4	200	BGP	0	1
10.0.4.0/24	10.0.1.200	port3	110	OSPF	2	1
10.0.4.0/24	10.0.2.200	port4	110	OSPF	2	1
10.200.1.0/24	0.0.0.0	port1	0	Connected	0	0
10.200.2.0/24	0.0.0.0	port2	0	Connected	0	0

```
# get router info routing-table all
…output omitted…
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 10.200.1.254, port1, [5/0]
                  [10/0] via 10.200.2.254, port2, [5/0]
C       10.0.1.0/24 is directly connected, port3
C       10.0.2.0/24 is directly connected, port4
B       10.0.3.0/24 [200/0] via 10.0.1.200 (recursive is directly connected, port3), 00:07:04, [1/0]
                    [200/0] via 10.0.2.200 (recursive is directly connected, port4), 00:07:04, [1/0]
O       10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:15:12, [1/0]
                    [110/2] via 10.0.2.200, port4, 00:15:12, [1/0]
C       10.200.1.0/24 is directly connected, port1
C       10.200.2.0/24 is directly connected, port2
```

The example on this slide shows two ECMP static routes, two ECMP BGP routes, and two ECMP OSPF routes. For each ECMP group, the destination subnet, distance, metric, and priority are the same. The result is that FortiGate installs both routes of each ECMP group in the routing table.

ECMP Load Balancing Algorithm



ECMP Load Balancing Algorithms

- Source IP (default)
  - Sessions sourced from the same address use the same route
- Source-destination IP
  - Sessions with the same source *and* destination address pair use the same route
- Weighted
  - Applies to static routes only
  - Sessions are distributed based on route, or interface weights
  - The higher the weight, the more sessions are routed through the selected route
- Usage (spillover)
  - One route is used until the bandwidth threshold is reached, then the next route is used

ECMP can load balance sessions using one of the following four algorithms:

- **Source IP: This is the default algorithm.** FortiGate uses the same ECMP route to route sessions sourced from the same address.

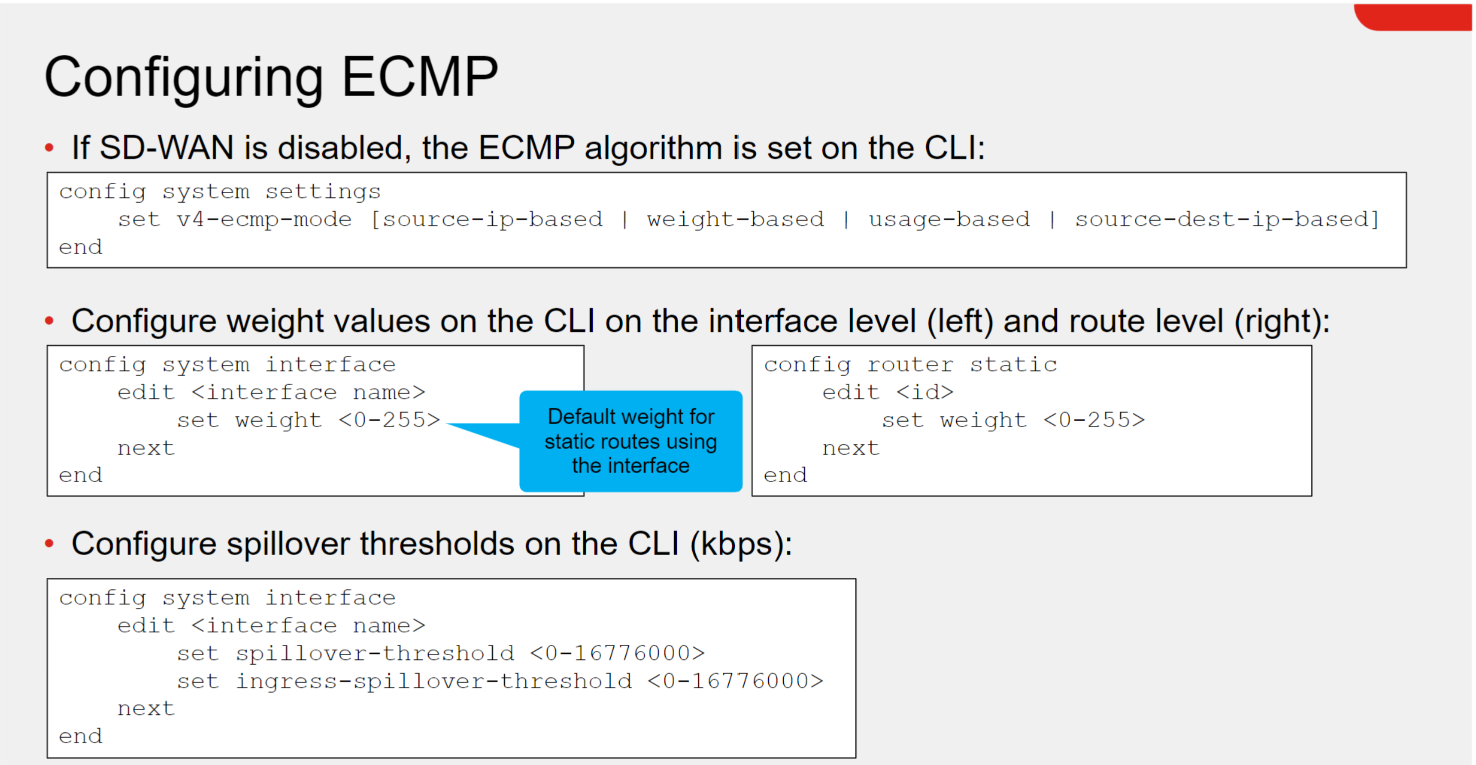
- **Source-destination IP:** FortiGate uses the same ECMP route to route sessions with the same source-destination IP address pair.

- **Weighted:** Applies to static routes only. FortiGate load balances sessions **based on the route weight or the respective interface weight**. **The higher the weight**, the more sessions FortiGate routes through the selected route.
  For a weighted algorithm, you must configure the weights *on the interface level* or *route level*.

The weight that you assign to each interface is used to calculate the percentage of the total sessions that are allowed to connect through an interface, and the sessions are distributed to the interfaces accordingly.

- **Usage (spillover):** FortiGate sends sessions to the interface of the first ECMP route until the bandwidth of the interface reaches the configured spillover limit. After the spillover limit is reached, FortiGate uses the interface of the next ECMP route.

Configuring ECMP



Configuring ECMP

- If SD-WAN is disabled, the ECMP algorithm is set on the CLI:

```
config system settings
    set v4-ecmp-mode [source-ip-based | weight-based | usage-based | source-dest-ip-based]
end
```

- Configure weight values on the CLI on the interface level (left) and route level (right):

```
config system interface
    edit <interface name>
        set weight <0-255>
    next
end
```

Default weight for static routes using the interface

```
config router static
    edit <id>
        set weight <0-255>
    next
end
```

- Configure spillover thresholds on the CLI (kbps):

```
config system interface
    edit <interface name>
        set spillover-threshold <0-16776000>
        set ingress-spillover-threshold <0-16776000>
    next
end
```

- **If SD-WAN is disabled**, you can change the ECMP load balancing algorithm on the FortiGate CLI using the commands shown on this slide.

- **When SD-WAN is enabled**, FortiOS hides the `v4-ecmp-mode` setting and replaces it with the `load-balance-mode` setting under `config system sdwan`. That is, when you enable SDWAN, you control the ECMP algorithm with the `load-balance-mode` setting.

- **For spillover to work**, you must also configure the egress and ingress spillover thresholds, as shown on this slide. The thresholds are set to 0 by default, which disables spillover check.

- **For a weighted algorithm**, you must configure the weights on the interface level or route level, as shown on this slide. If two or more routes are added to the routing table, and you set **v4-ecmp-mode** to **weight-based**, FortiGate routes sessions based on the weight value of each route in the percentage value.

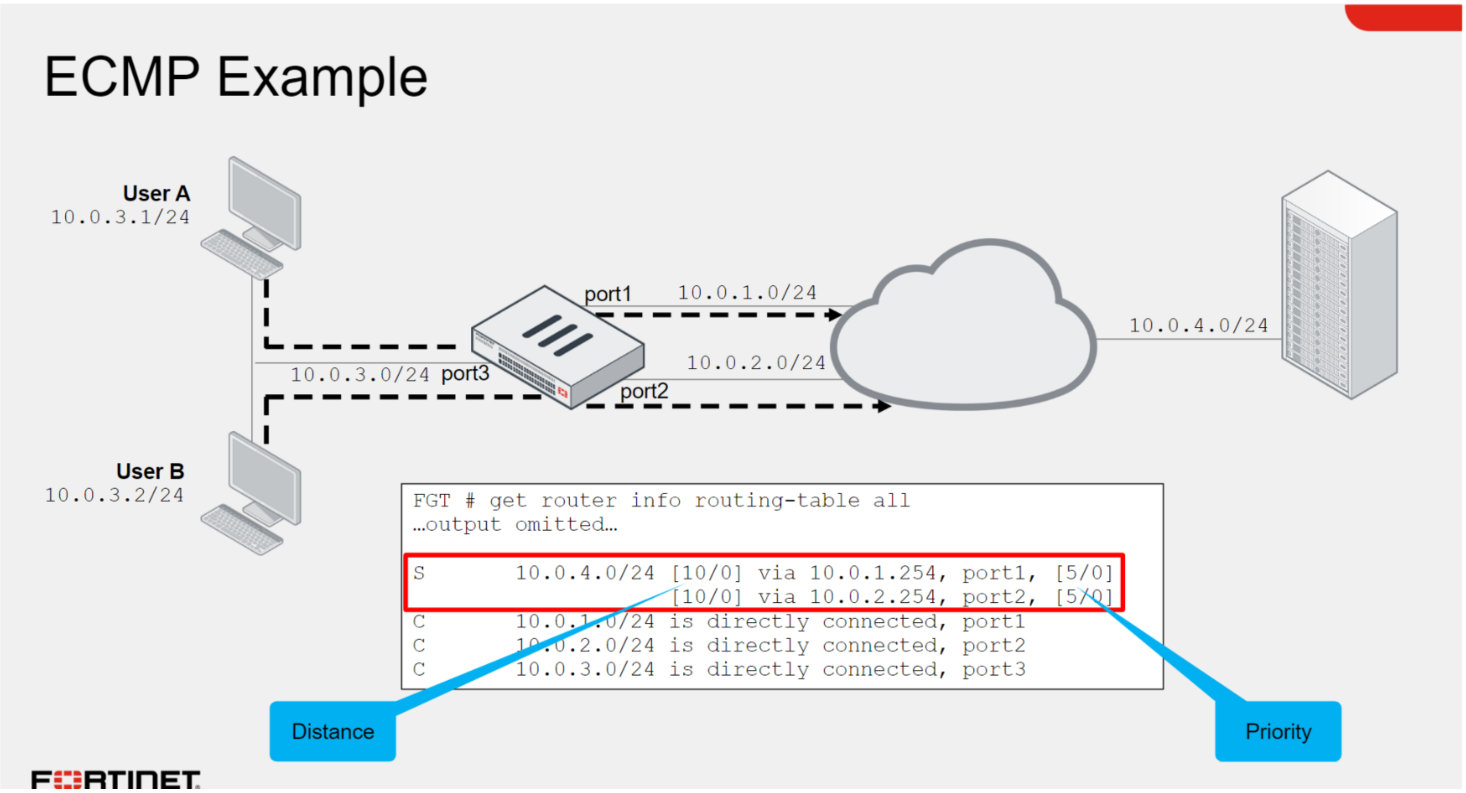
To change the number of paths allowed by ECMP:

```
config system settings

set ecmp-max-paths <number of paths>

end
```

Setting ecmp-max-paths to the lowest value of 1 is equivalent to disabling ECMP.

ECMP Examples

Example 1:



ECMP Example

```
FGT # get router info routing-table all
…output omitted…

S       10.0.4.0/24 [10/0] via 10.0.1.254, port1, [5/0]
                    [10/0] via 10.0.2.254, port2, [5/0]
C       10.0.1.0/24 is directly connected, port1
C       10.0.2.0/24 is directly connected, port2
C       10.0.3.0/24 is directly connected, port3
```

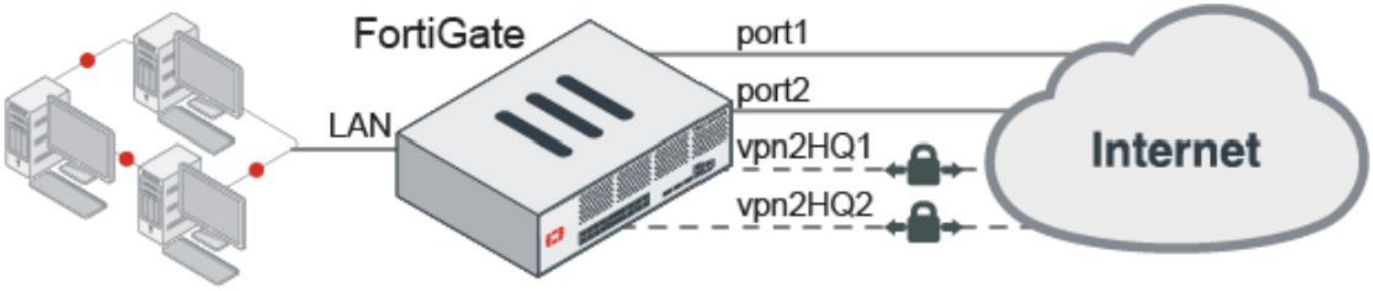
In the scenario shown on this slide, FortiGate has ECMP routes for the 10.0.4.0/24 subnet on port1 and port2. Using the default ECMP algorithm (source IP based), FortiGate may use any of the two routes to route traffic from user A and user B.

In the example shown on this slide, FortiGate selects the route over port1 for user A, and the route over port2 for user B. FortiGate continues to use the same selected routes for the same traffic. In the route over port1 is removed from the routing table, FortiGate automatically starts to forward the traffic sourced from both users and destined to 10.0.4.0/24 through port2.

ECMP enables you to use multiple paths for the same destination, as well as provide built-in failover. Usually, you want to use ECMP for mission-critical services that require high availability. Another reason to use ECMP is for bandwidth aggregation. That is, you can leverage the bandwidth of multiple links by load balancing sessions across them.

While ECMP enables you to leverage multiple WAN links on FortiGate, you may want to use SD-WAN because of the additional benefits.

Example 2:



Example 1: Default ECMP

```
config router static
    edit 1
        set gateway 172.16.151.1
        set device "port1"
    next
    edit 2
        set gateway 192.168.2.1
        set device "port2"
    next
end
# get router info routing-table all
Routing table for VRF=0
S*    0.0.0.0/0 [10/0] via 172.16.151.1, port1
                [10/0] via 192.168.2.1, port2
C    172.16.151.0/24 is directly connected, port1
C    192.168.2.0/24 is directly connected, port2
```

Result:

Both routes are added to the routing table and load-balanced based on the source IP.

Example 2: Same distance, different priority

```
config router static
    edit 1
        set gateway 172.16.151.1
        set priority 5
        set device "port1"
    next
    edit 2
        set gateway 192.168.2.1
        set device "port2"
    next
end
# get router info routing-table all
Routing table for VRF=0
S*    0.0.0.0/0 [10/0] via 192.168.2.1, port2
                [10/0] via 172.16.151.1, port1, [5/0]
C    172.16.151.0/24 is directly connected, port1
C    192.168.2.0/24 is directly connected, port2
```

Result:

Both routes are added to the routing table, but traffic is routed to port2 which has a lower priority value with a default of 0.

Example 3: Weight-based ECMP

```
config router static
    edit 3
        set dst 10.10.30.0 255.255.255.0
        set weight 80
        set device "vpn2HQ1"
    next
    edit 5
        set dst 10.10.30.0 255.255.255.0
        set weight 20
        set device "vpn2HQ2"
    next
end Copy
# get router info routing-table all
Routing table for VRF=0
...
S    10.10.30.0/24 [10/0] is directly connected, vpn2HQ1, [0/80]
                   [10/0] is directly connected, vpn2HQ2, [0/20]
C    172.16.151.0/24 is directly connected, port1
C    192.168.0.0/24 is directly connected, port3
C    192.168.2.0/24 is directly connected, port2
```

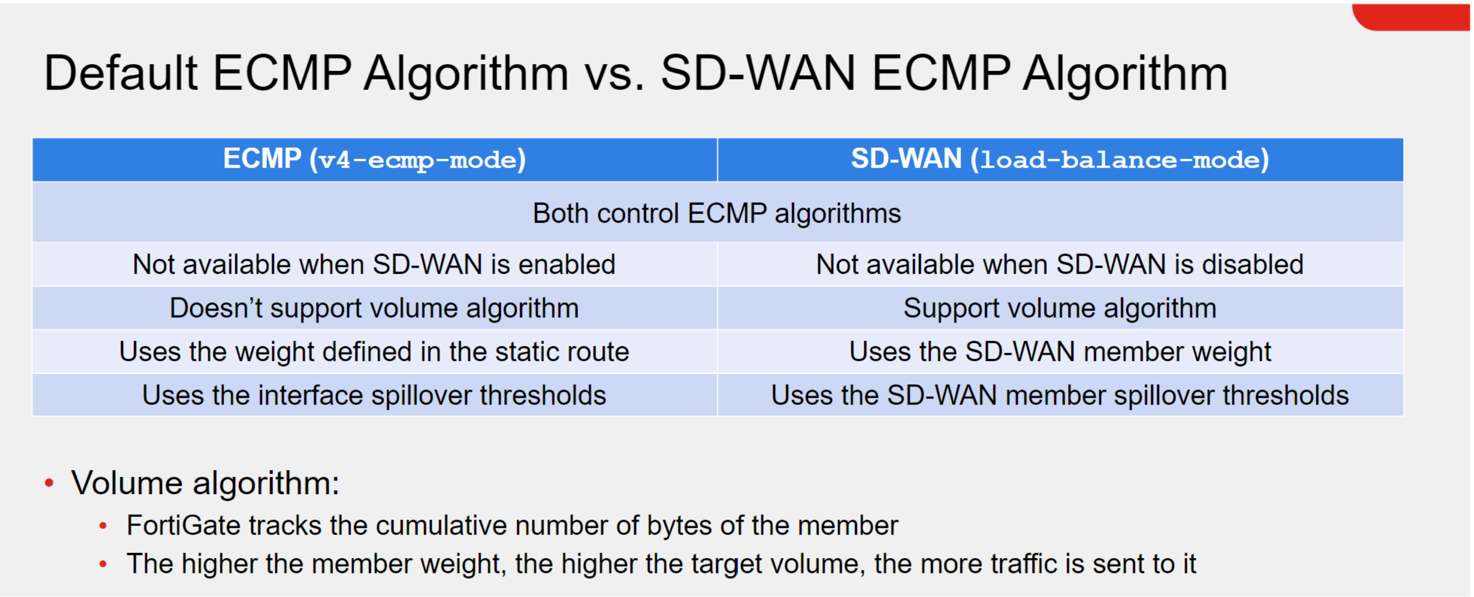
Result:

Both routes are added to the routing table, but 80% of the sessions to 10.10.30.0/24 are routed to vpn2HQ1, and 20% are routed to vpn2HQ2.

Default ECMP Algorithm

vs.

SD-WAN ECMP Algorithm



Default ECMP Algorithm vs. SD-WAN ECMP Algorithm

ECMP (`v4-ecmp-mode`)	SD-WAN (`load-balance-mode`)
Both control ECMP algorithms	
Not available when SD-WAN is enabled	Not available when SD-WAN is disabled
Doesn't support volume algorithm	Support volume algorithm
Uses the weight defined in the static route	Uses the SD-WAN member weight
Uses the interface spillover thresholds	Uses the SD-WAN member spillover thresholds

- Volume algorithm:
  - FortiGate tracks the cumulative number of bytes of the member
  - The higher the member weight, the higher the target volume, the more traffic is sent to it

When you enable SD-WAN, FortiOS hides the `v4-ecmp-mode` setting and replaces it with the `load-balance-mode` setting under `config system sdwan`. That is, after you enable SDWAN, you now control the ECMP algorithm with the `load-balance-mode` setting.

There are some differences between the two settings:

- The main difference is that `load-balance-mode` supports the **volume algorithm**, and `v4-ecmp-mode` does not.
- In addition, the related settings such as weight and spillover thresholds are configured differently. That is, when you enable SD-WAN, the weight and spillover thresholds are defined on the SD-WAN member configuration. When you disable SDWAN, the weight and spillover thresholds are defined on the static route and interface settings, respectively.

When you set the ECMP algorithm to volume— this is when SD-WAN is enabled, FortiGate load balances sessions across members based on the measured interface volume and the member weight. That is, the volume algorithm instructs FortiGate to track the cumulative number of bytes of each member and to distribute sessions based on the weight. The higher the weight, the higher the target volume of the interface and, as a result, the more traffic FortiGate sends to it.

ECMP	SD-WAN		Description
	GUI	CLI	
source-ip-based	Source IP	source-ip-based	Traffic is divided equally between the interfaces. Sessions that start at the same source IP address use the same path. This is the default selection.
weight-based	Sessions	weight-based	The workload is distributed based on the number of sessions that are connected through the interface. The weight that you assign to each interface is used to calculate the percentage of the total sessions allowed to connect through an interface, and the sessions are distributed to the interfaces accordingly.
usage-based	Spillover	usage-based	The interface is used until the traffic bandwidth exceeds the ingress and egress thresholds that you set for that interface. Additional traffic is then sent through the next interface member.
source-dest-ip-based	Source-Destination IP	source-dest-ip-based	Traffic is divided equally between the interfaces. Sessions that start at the same source IP address and go to the same destination IP address use the same path.
Not supported	Volume	measured-volume-based	This mode is supported in SD-WAN only. The workload is distributed based on the number of packets that are going through the interface.

LAB

In this lab, you will configure the router settings and test scenarios to learn how FortiGate makes routing decisions.

Objectives

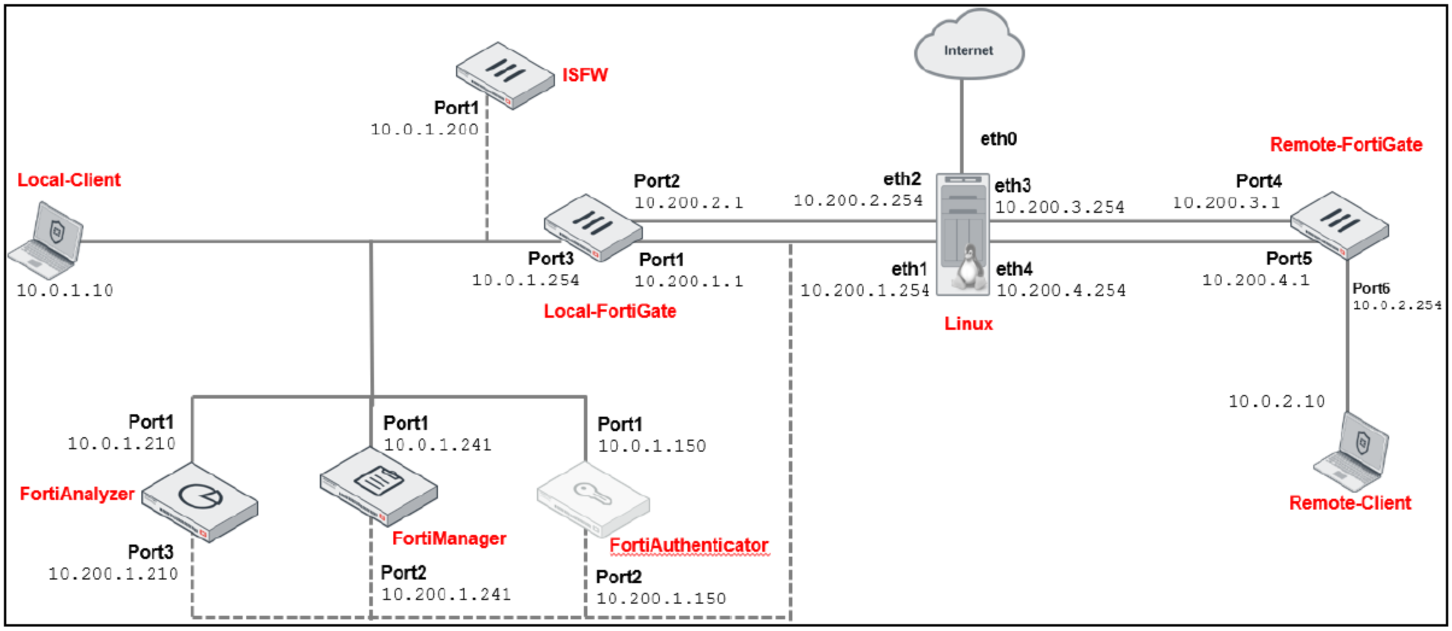
- Route traffic based on the destination IP address, as well as other criteria
- Balance traffic among multiple paths
- Implement route failover
- Diagnose a routing problem

We have two exercises in this LAB:

Exercise 1: Configuring Route Failover

Exercise 2: Configuring Equal-Cost Multi-Path Routing

LAB Topology:



Exercise 1: Configuring Route Failover

In the lab network, Local-FortiGate has two interfaces connected to the internet: port1 and port2. In this exercise, you will configure the port1 connection as the primary internet link and the port2 connection as the backup internet link. Local-FortiGate should use the port2 connection only if the port1 connection is down. To achieve this objective, you will configure two default routes with different administrative distances, and then you will disable the primary default route interface to activate the standby route.

Verify the Routing Configuration

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

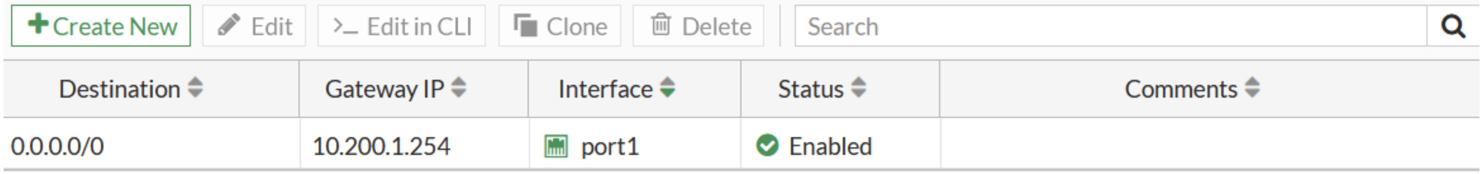
> **Take the Expert Challenge!**
>
> On the Local-FortiGate GUI (admin/password), complete the following:
>
> - View the existing static route configuration on Local-FortiGate.
> - Enable the **Distance** and **Priority** columns on the static route configuration page.
> - Make a note of the **Distance** and **Priority** values of the existing default route.
>
> If you require assistance, or to verify your work, use the step-by-step instructions that follow.

To verify the routing configuration

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.

2. Click **Network** > **Static Routes**.

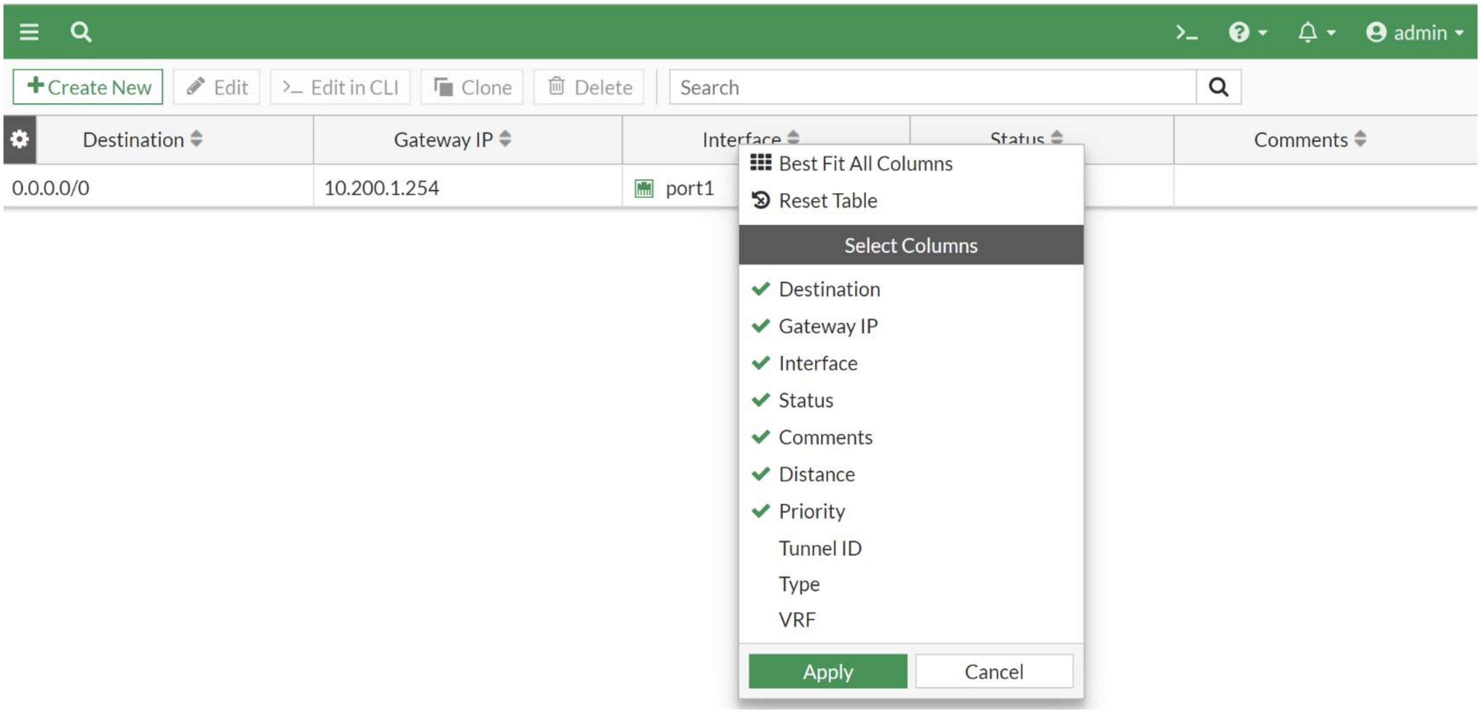
3. Verify the existing default route for **port1**.



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**.



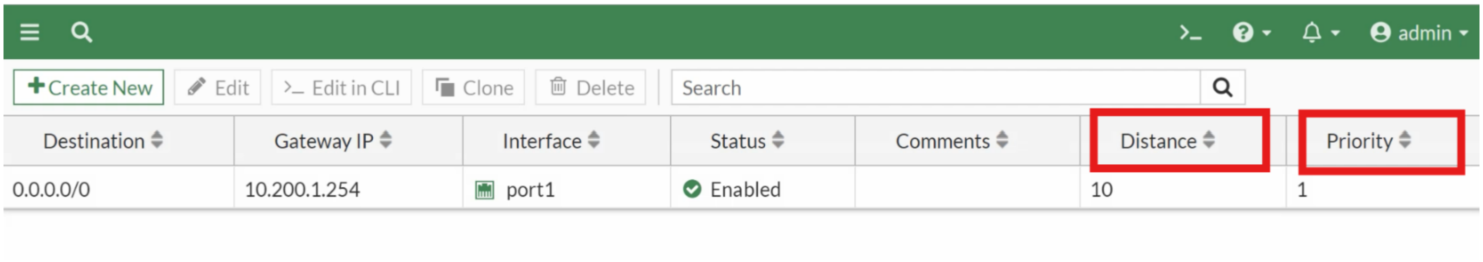
Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	10.200.1.254	port1		

Select Columns

- ✓ Destination
- ✓ Gateway IP
- ✓ Interface
- ✓ Status
- ✓ Comments
- ✓ Distance
- ✓ Priority
- Tunnel ID
- Type
- VRF

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.



Destination	Gateway IP	Interface	Status	Comments	Distance	Priority
0.0.0.0/0	10.200.1.254	port1	Enabled		10	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.

Take the Expert Challenge!

- On the Local-FortiGate GUI, configure a second default route using **port2**.
- Assign it a **Distance** of 20 and a **Priority** of 5.

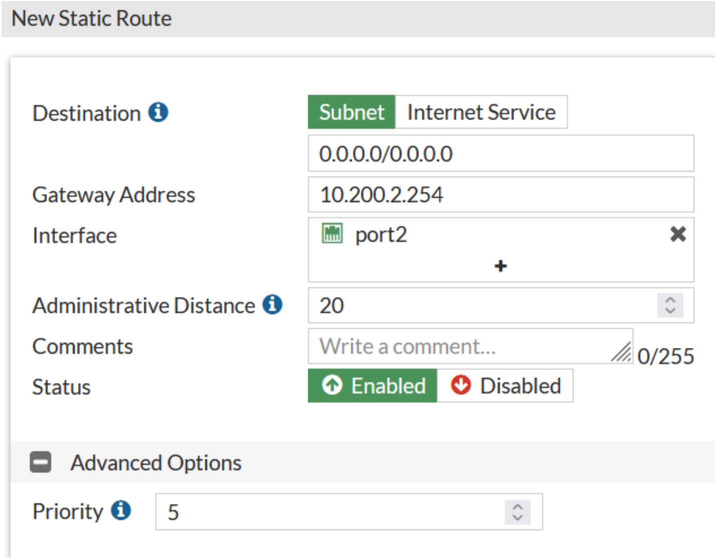
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

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

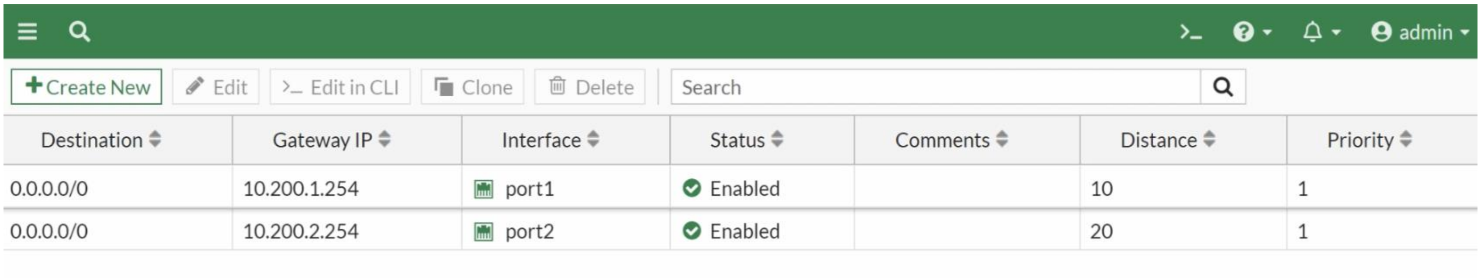
Destination: Subnet | Internet Service
0.0.0.0/0.0.0.0
Gateway Address: 10.200.2.254
Interface: port2
Administrative Distance: 20
Comments: Write a comment... 0/255
Status: Enabled | Disabled

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	10.200.1.254	port1	✓ Enabled		10	1
0.0.0.0/0	10.200.2.254	port2	✓ Enabled		20	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.

Take the Expert Challenge!

- Continuing on the Local-FortiGate GUI, enable logging for all sessions in the existing **Full_Access** firewall policy.
- Create a second firewall policy named Backup_Access.
- Configure the **Backup_Access** policy to allow traffic from **port3** to **port2** with NAT enabled.
- Enable logging on the **Backup_Access** policy for all sessions.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

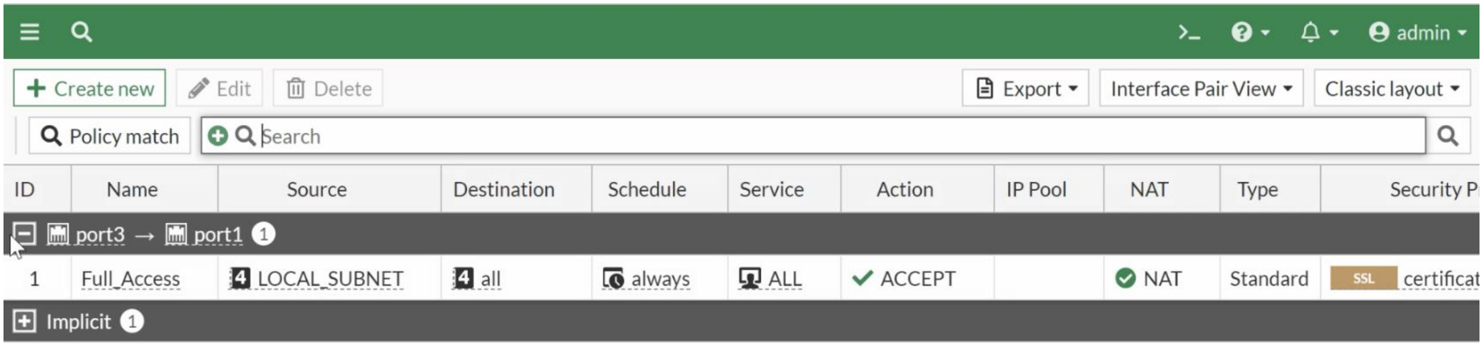
To configure the firewall policies

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.

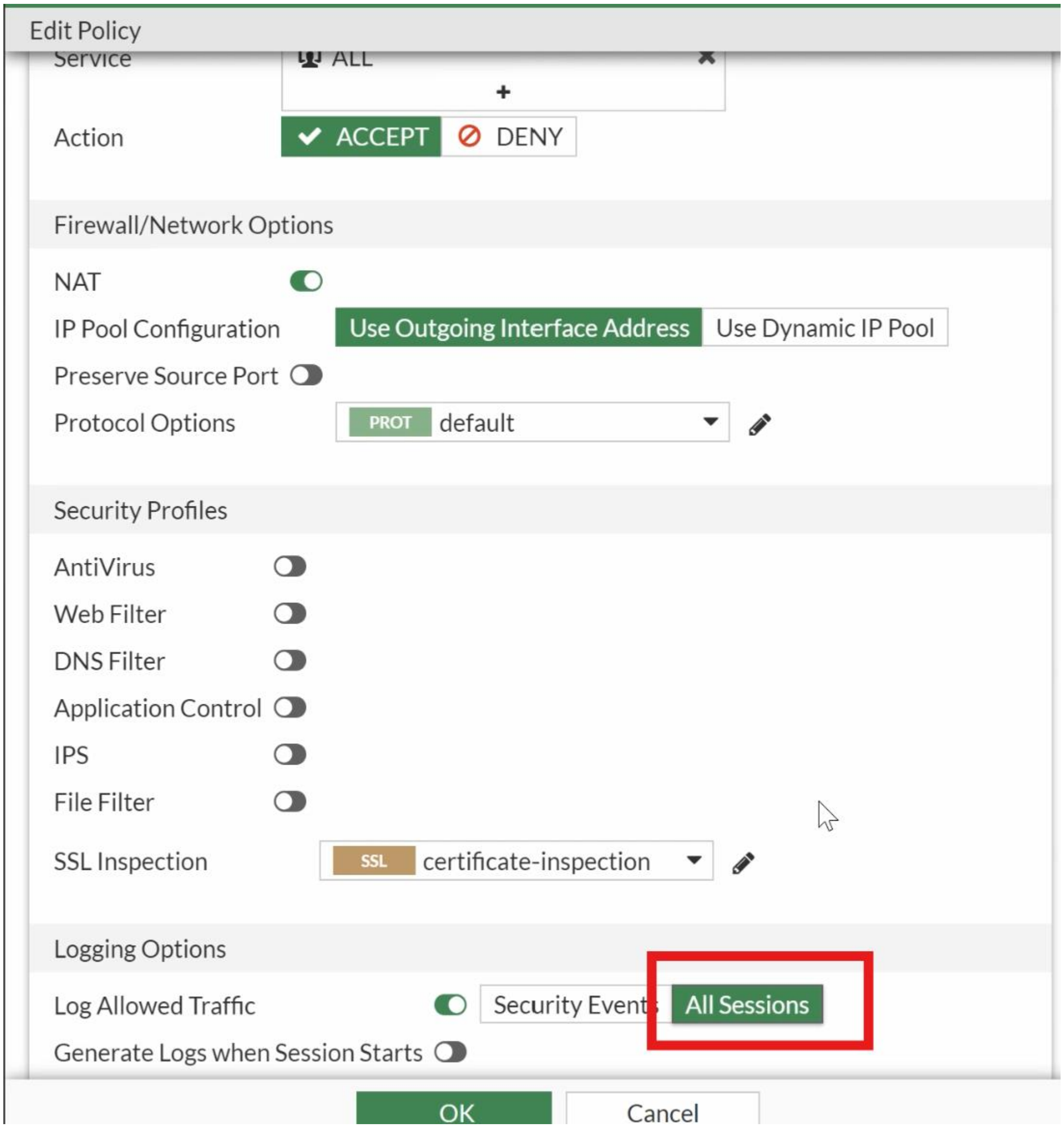
2. Double-click the existing **Full_Access** policy to edit it.

3. Enable **Log Allowed Traffic**, and then select **All Sessions**.

All Sessions logging ensures that FortiGate logs all traffic, not only sessions that security profiles inspected. This will assist you in verifying traffic routing using the **Forward Traffic** logs.



ID	Name	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security P
port3 → port1 1										
1	Full_Access	LOCAL_SUBNET	all	always	ALL	✓ ACCEPT		✓ NAT	Standard	SSL certificat
Implicit 1										



Service ALL

Action [✓ ACCEPT] DENY

Firewall/Network Options

NAT ●

IP Pool Configuration [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Preserve Source Port ○

Protocol Options PROT default

Security Profiles

AntiVirus ○

Web Filter ○

DNS Filter ○

Application Control ○

IPS ○

File Filter ○

SSL Inspection SSL certificate-inspection

Logging Options

Log Allowed Traffic ● Security Events [✓ All Sessions]

Generate Logs when Session Starts ○

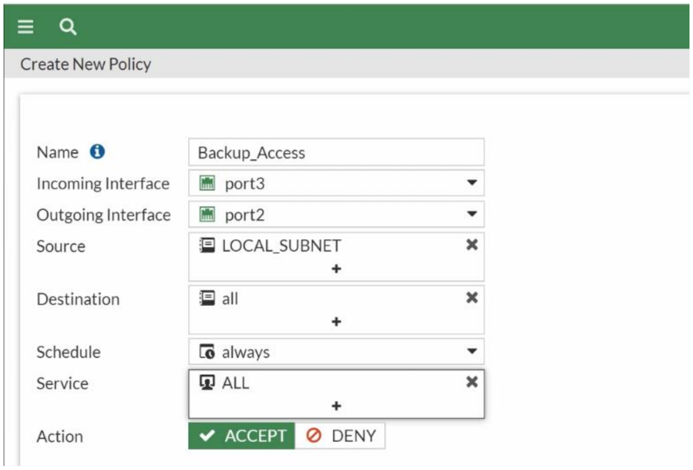
4. Click **OK**.

5. Click **Create New**.

6. Configure a second firewall policy with the following settings:

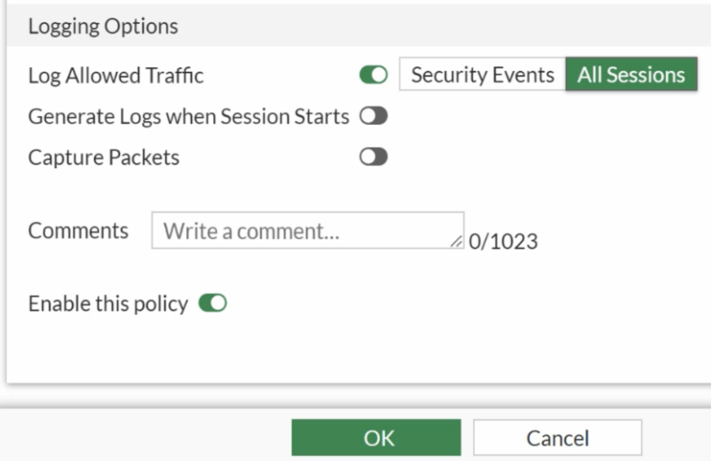
Field	Value
Name	Backup_Access
Incoming Interface	port3
Outgoing Interface	port2
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Log Allowed Traffic	All Sessions

7. Click **OK**.



Create New Policy

Name	Backup_Access
Incoming Interface	port3
Outgoing Interface	port2
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY



Logging Options

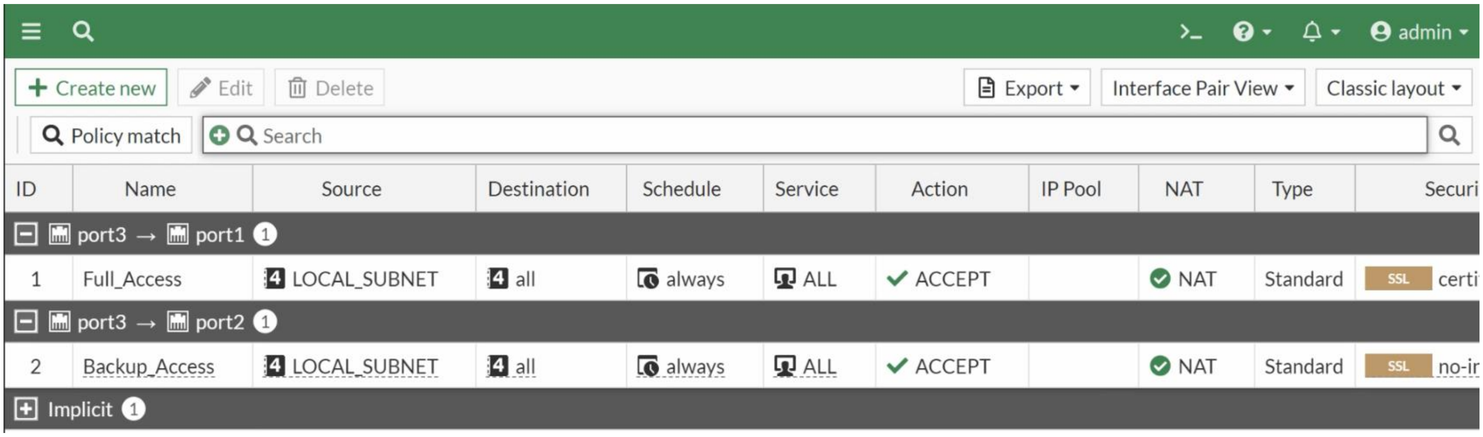
Log Allowed Traffic ● Security Events **All Sessions**

Generate Logs when Session Starts ○

Capture Packets ○

Comments Write a comment... 0/1023

Enable this policy ●



ID	Name	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Securi
⊟ port3 → port1 1										
1	Full_Access	LOCAL_SUBNET	all	always	ALL	✓ ACCEPT		NAT	Standard	SSL certi
⊟ port3 → port2 1										
2	Backup_Access	LOCAL_SUBNET	all	always	ALL	✓ ACCEPT		NAT	Standard	SSL no-ir
⊞ Implicit 1										

View the Routing Table

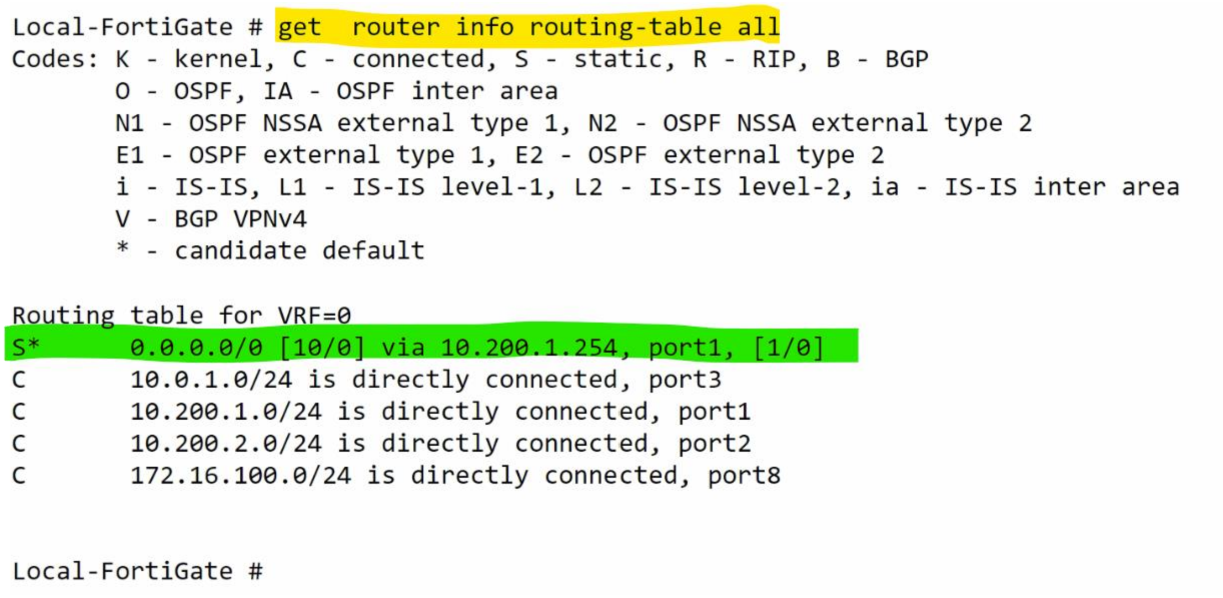
The Local-FortiGate configuration now has two default routes with different distances. You will view the routing table to see which route was installed in the routing table and which route was installed in the routing table database.

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
   ```



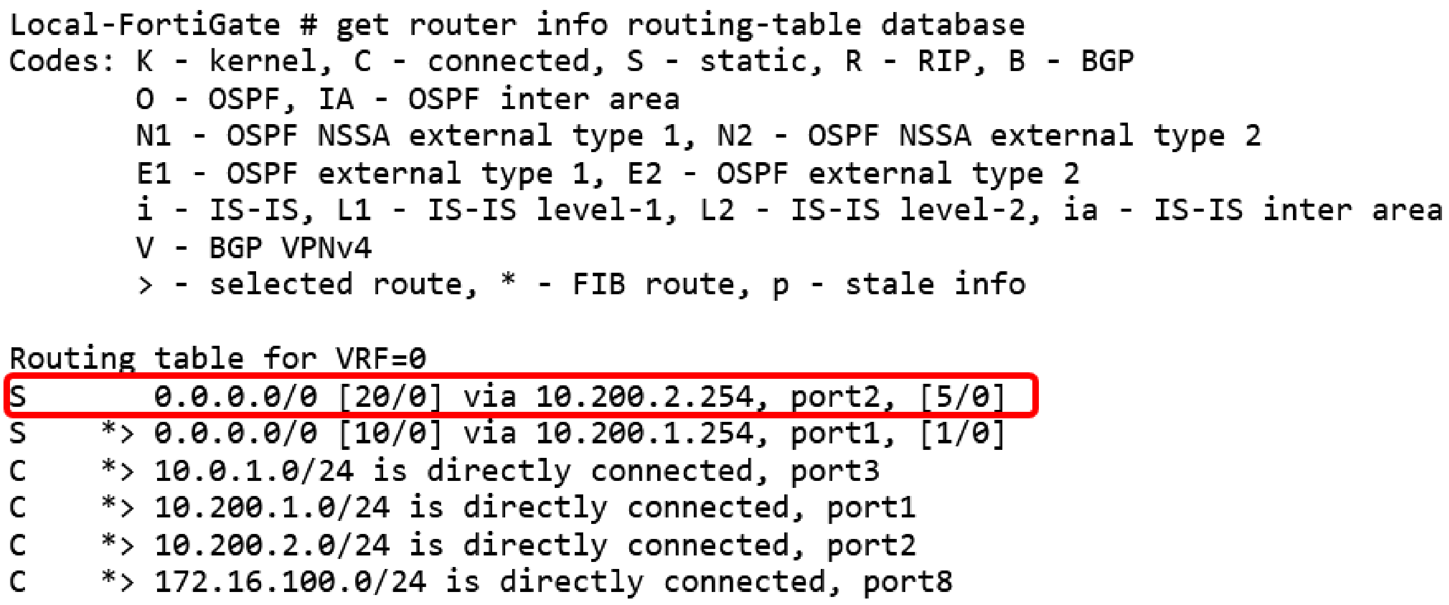
```
Local-FortiGate # get  router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS,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

Routing table for VRF=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


Local-FortiGate #
```

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
```

Only active routes show the > symbol, which means they are the selected and active routes. The routing table database contains all active, standby, and inactive routes on FortiGate.

Stop and think!

Why is the port2 default route the standby route?

The port2 default route has a higher administrative distance than the port1 default route. When two or more routes to the same destination have different distances, the higher distance route is not installed in the routing table, but you can still see it in the routing table database. Routes marked as inactive are marked inactive when the corresponding interface is down.

5. Close the Local-FortiGate CLI session.

Test the Route Failover

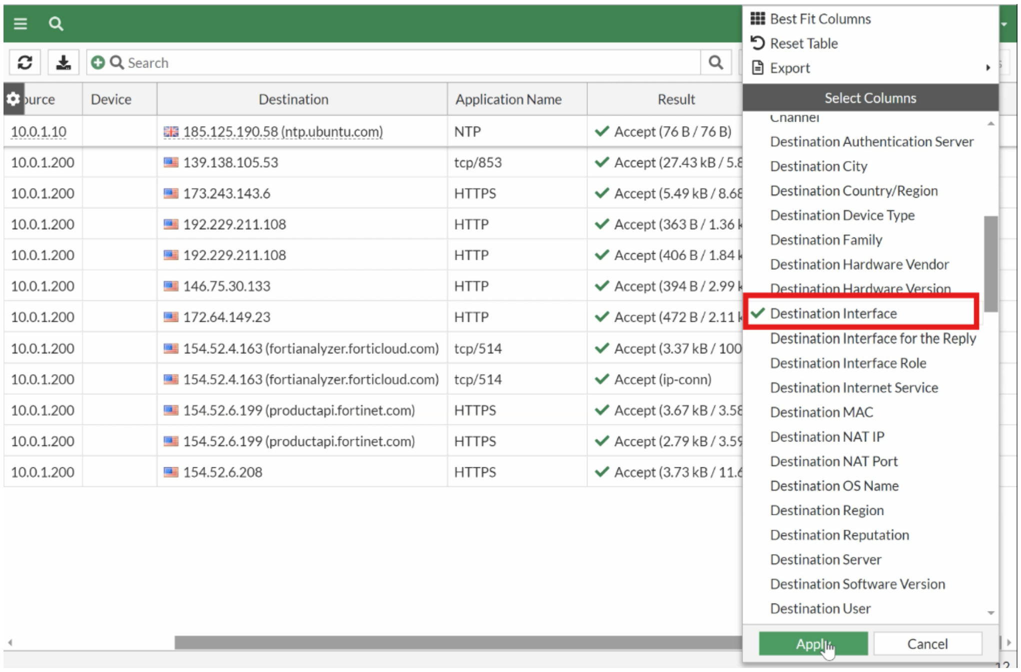
First, you will access various websites and use the **Forward Traffic** logs to verify that the port1 route is being used. Next, you will force a failover by reconfiguring the port1 interface setting and bringing the interface down. You will then generate some more traffic, and use the **Forward Traffic**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

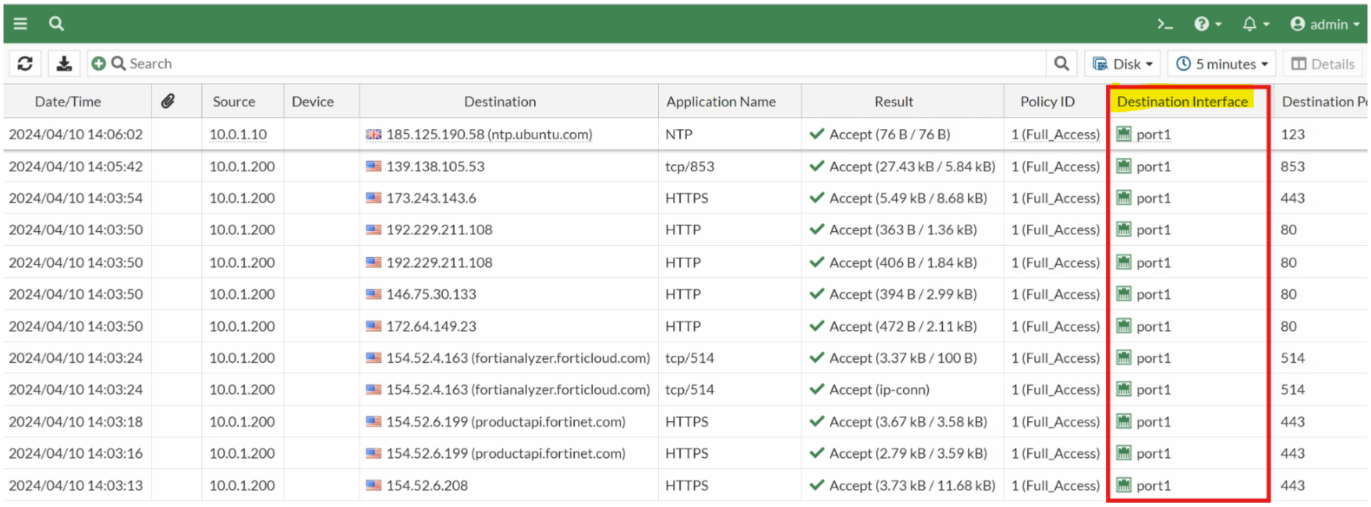
3. In the **Select Columns** section, select **Destination Interface**.



urce	Device	Destination	Application Name	Result
10.0.1.10		185.125.190.58 (ntp.ubuntu.com)	NTP	✓ Accept (76 B / 76 B)
10.0.1.200		139.138.105.53	tcp/853	✓ Accept (27.43 kB / 5.8
10.0.1.200		173.243.143.6	HTTPS	✓ Accept (5.49 kB / 8.68
10.0.1.200		192.229.211.108	HTTP	✓ Accept (363 B / 1.36 k
10.0.1.200		192.229.211.108	HTTP	✓ Accept (406 B / 1.84 k
10.0.1.200		146.75.30.133	HTTP	✓ Accept (394 B / 2.99 k
10.0.1.200		172.64.149.23	HTTP	✓ Accept (472 B / 2.11 k
10.0.1.200		154.52.4.163 (fortianalyzer.forticloud.com)	tcp/514	✓ Accept (3.37 kB / 100
10.0.1.200		154.52.4.163 (fortianalyzer.forticloud.com)	tcp/514	✓ Accept (ip-conn)
10.0.1.200		154.52.6.199 (productapi.fortinet.com)	HTTPS	✓ Accept (3.67 kB / 3.58
10.0.1.200		154.52.6.199 (productapi.fortinet.com)	HTTPS	✓ Accept (2.79 kB / 3.59
10.0.1.200		154.52.6.208	HTTPS	✓ Accept (3.73 kB / 11.6

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

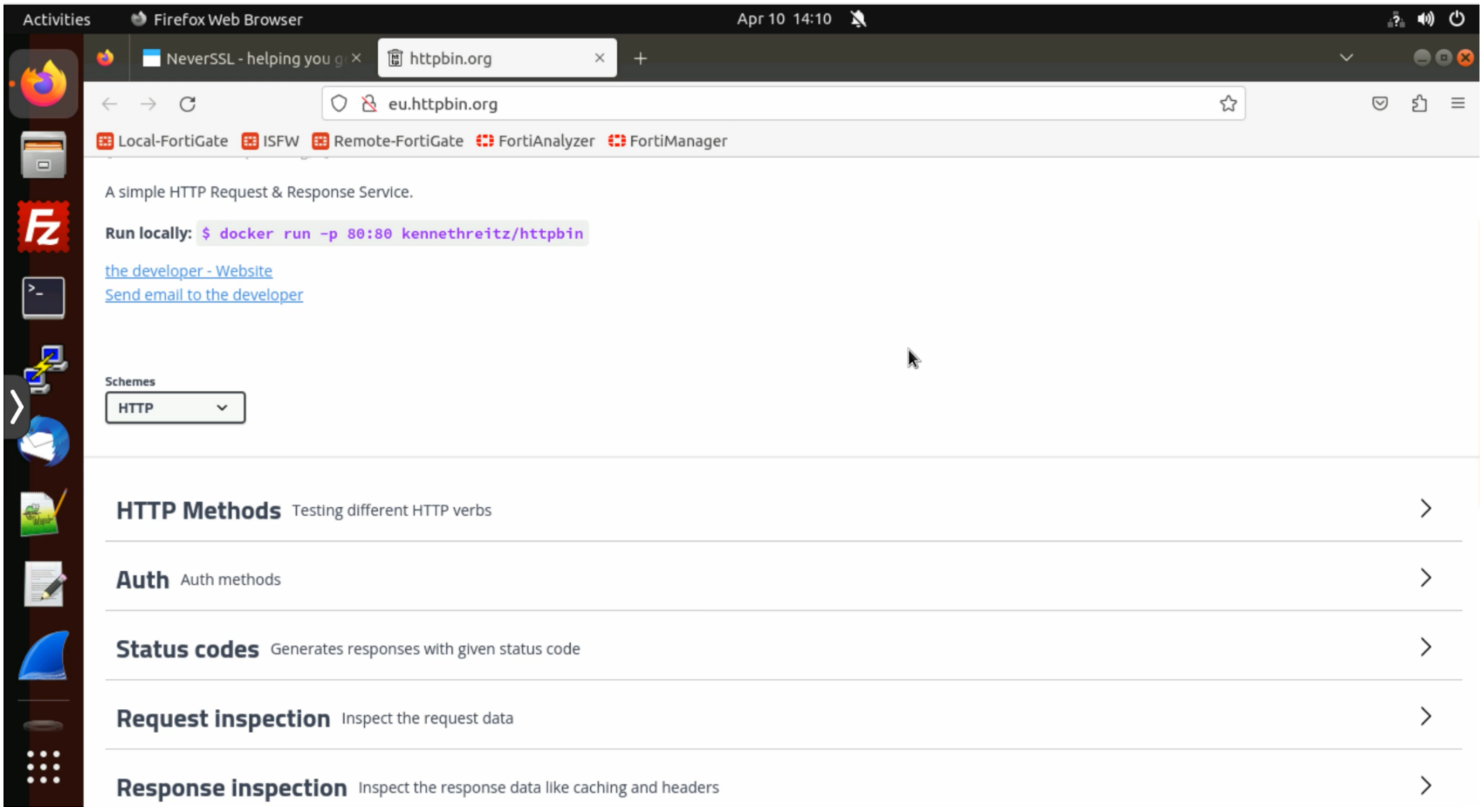
The **Destination Interface** column is displayed.



Date/Time	📎	Source	Device	Destination	Application Name	Result	Policy ID	Destination Interface	Destination P
2024/04/10 14:06:02		10.0.1.10		185.125.190.58 (ntp.ubuntu.com)	NTP	✓ Accept (76 B / 76 B)	1 (Full_Access)	port1	123
2024/04/10 14:05:42		10.0.1.200		139.138.105.53	tcp/853	✓ Accept (27.43 kB / 5.84 kB)	1 (Full_Access)	port1	853
2024/04/10 14:03:54		10.0.1.200		173.243.143.6	HTTPS	✓ Accept (5.49 kB / 8.68 kB)	1 (Full_Access)	port1	443
2024/04/10 14:03:50		10.0.1.200		192.229.211.108	HTTP	✓ Accept (363 B / 1.36 kB)	1 (Full_Access)	port1	80
2024/04/10 14:03:50		10.0.1.200		192.229.211.108	HTTP	✓ Accept (406 B / 1.84 kB)	1 (Full_Access)	port1	80
2024/04/10 14:03:50		10.0.1.200		146.75.30.133	HTTP	✓ Accept (394 B / 2.99 kB)	1 (Full_Access)	port1	80
2024/04/10 14:03:50		10.0.1.200		172.64.149.23	HTTP	✓ Accept (472 B / 2.11 kB)	1 (Full_Access)	port1	80
2024/04/10 14:03:24		10.0.1.200		154.52.4.163 (fortianalyzer.forticloud.com)	tcp/514	✓ Accept (3.37 kB / 100 B)	1 (Full_Access)	port1	514
2024/04/10 14:03:24		10.0.1.200		154.52.4.163 (fortianalyzer.forticloud.com)	tcp/514	✓ Accept (ip-conn)	1 (Full_Access)	port1	514
2024/04/10 14:03:18		10.0.1.200		154.52.6.199 (productapi.fortinet.com)	HTTPS	✓ Accept (3.67 kB / 3.58 kB)	1 (Full_Access)	port1	443
2024/04/10 14:03:16		10.0.1.200		154.52.6.199 (productapi.fortinet.com)	HTTPS	✓ Accept (2.79 kB / 3.59 kB)	1 (Full_Access)	port1	443
2024/04/10 14:03:13		10.0.1.200		154.52.6.208	HTTPS	✓ Accept (3.73 kB / 11.68 kB)	1 (Full_Access)	port1	443

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



A simple HTTP Request & Response Service.

Run locally: `$ docker run -p 80:80 kennethreitz/httpbin`

the developer - Website
Send email to the developer

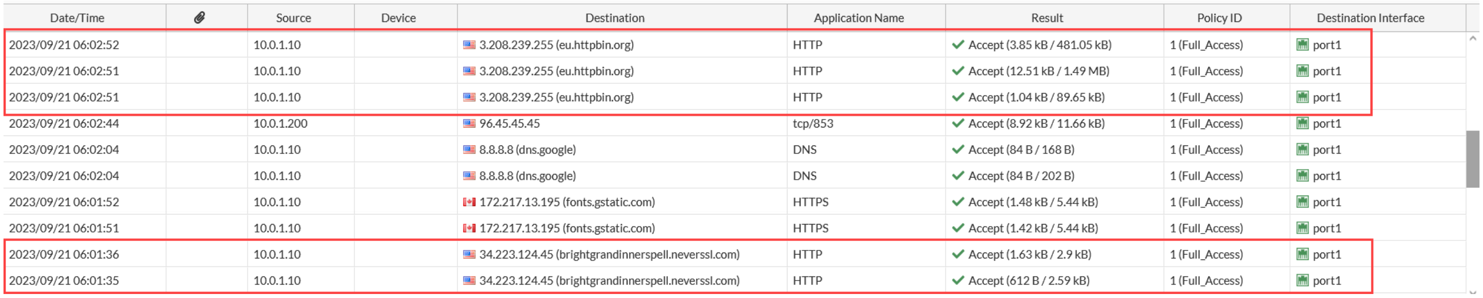
Schemes: HTTP

Activities
Firefox Web Browser
Apr 10 14:10
NeverSSL - helping you g
httpbin.org
eu.httpbin.org
Local-FortiGate
ISFW
Remote-FortiGate
FortiAnalyzer
FortiManager
HTTP Methods Testing different HTTP verbs
Auth Auth methods
Status codes Generates responses with given status code
Request inspection Inspect the request data
Response inspection Inspect the response data like caching and headers

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**.

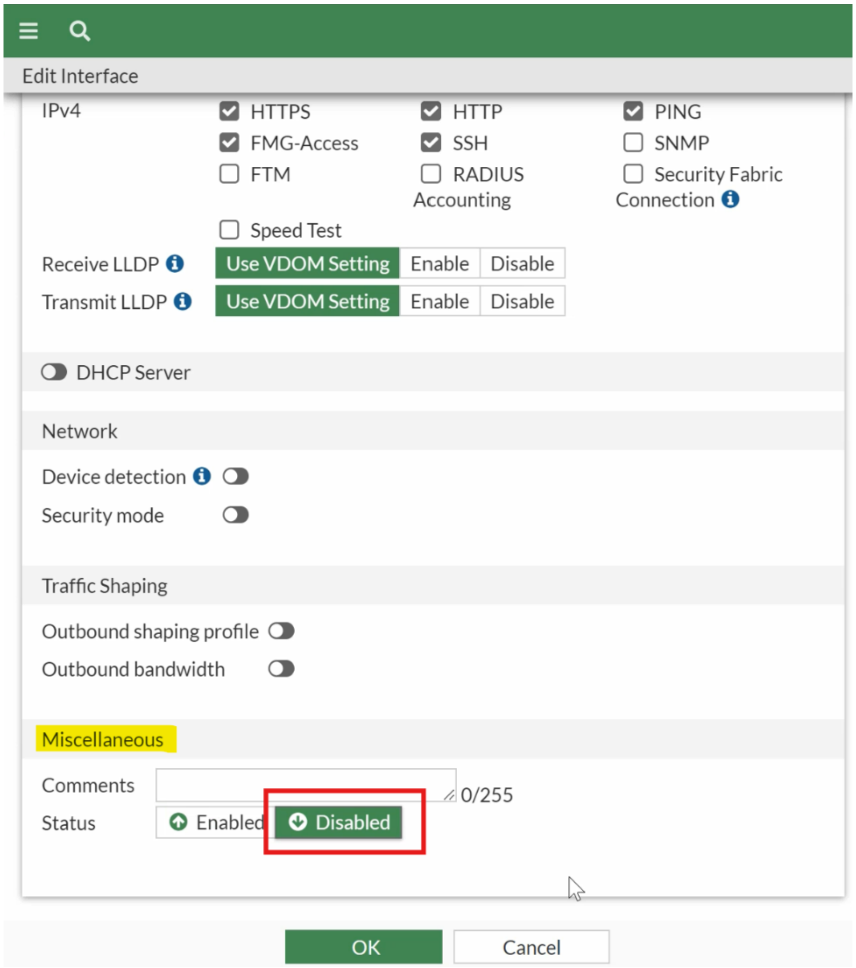


Date/Time		Source	Device	Destination	Application Name	Result	Policy ID	Destination Interface
2023/09/21 06:02:52		10.0.1.10		3.208.239.255 (eu.httpbin.org)	HTTP	✓ Accept (3.85 kB / 481.05 kB)	1 (Full_Access)	port1
2023/09/21 06:02:51		10.0.1.10		3.208.239.255 (eu.httpbin.org)	HTTP	✓ Accept (12.51 kB / 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**.



Edit Interface

IPv4: ☑ HTTPS ☑ HTTP ☑ PING ☑ FMG-Access ☑ SSH ☐ SNMP ☐ FTM ☐ RADIUS Accounting ☐ Security Fabric Connection ☐ Speed Test

Receive LLDP: Use VDOM Setting | Enable | Disable

Transmit LLDP: Use VDOM Setting | Enable | Disable

DHCP Server

Network

Device detection

Security mode

Traffic Shaping

Outbound shaping profile

Outbound bandwidth

Miscellaneous

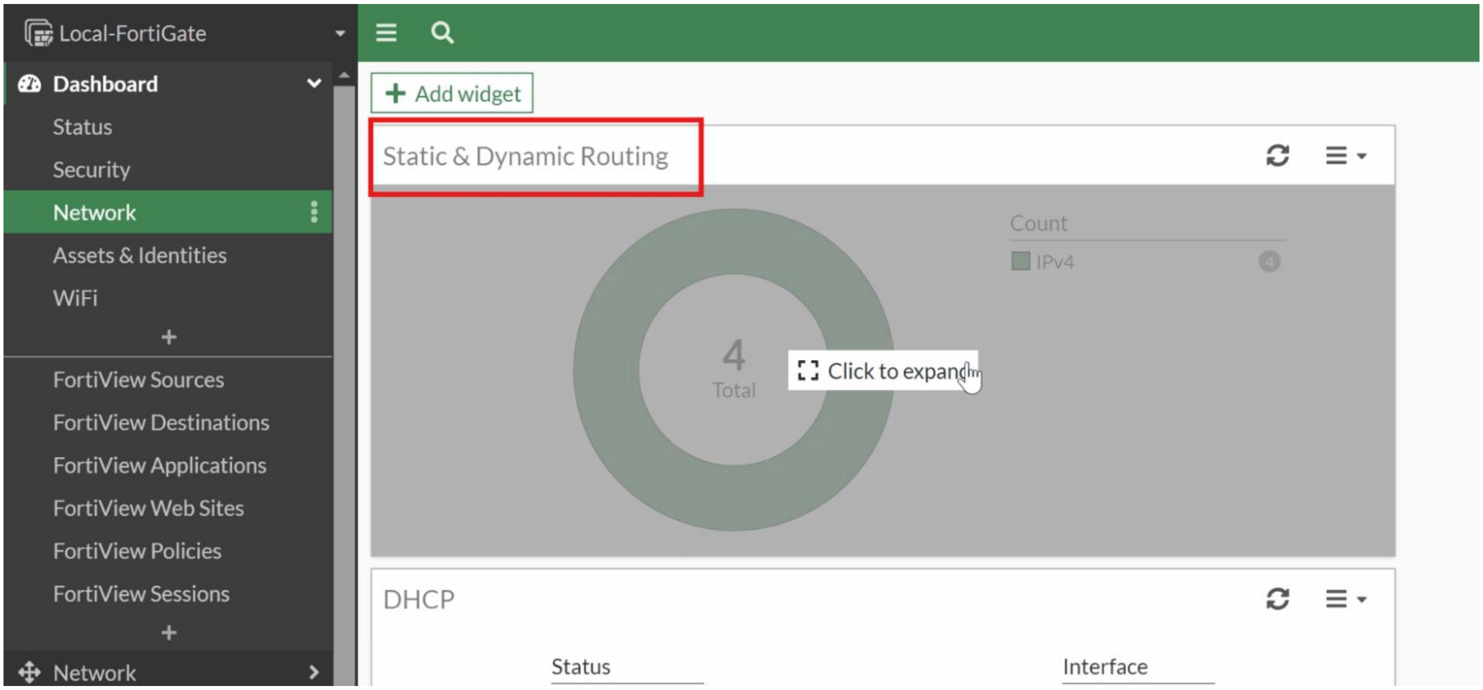
Comments: 0/255

Status: Enabled | Disabled

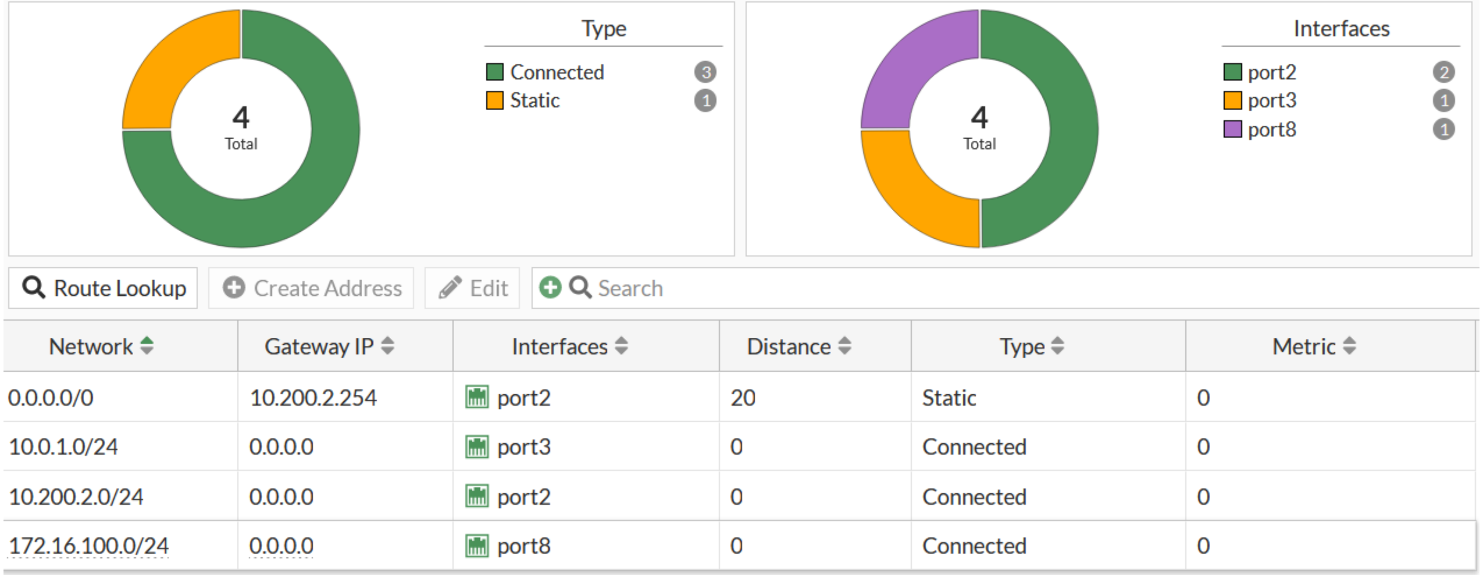
The port1 internet connection is now down, and FortiGate removes the corresponding route from the routing table.

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

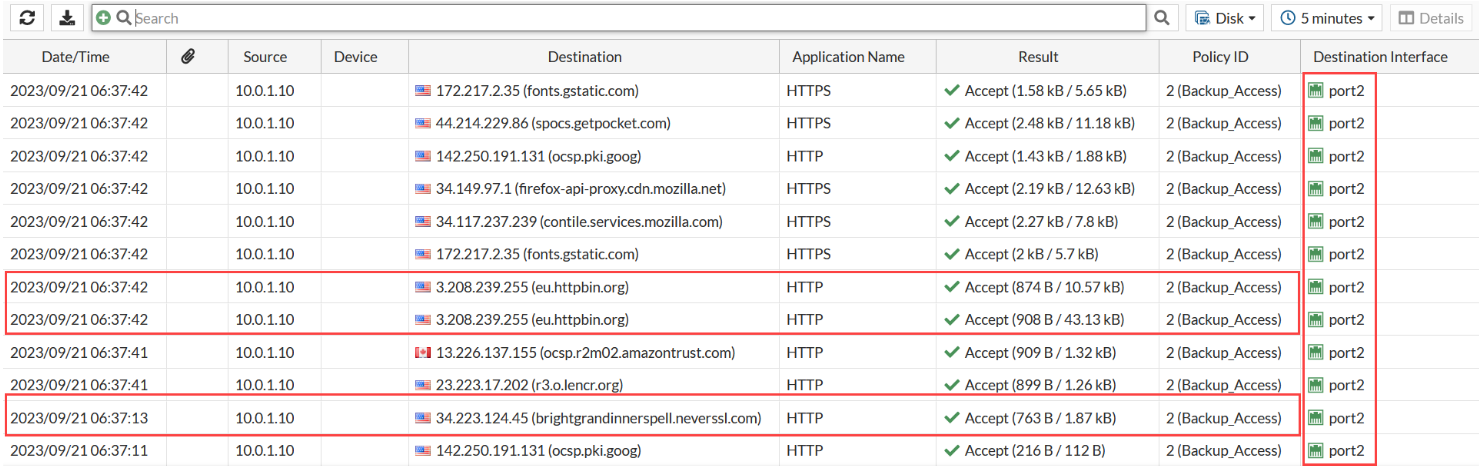
To verify traffic logs

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

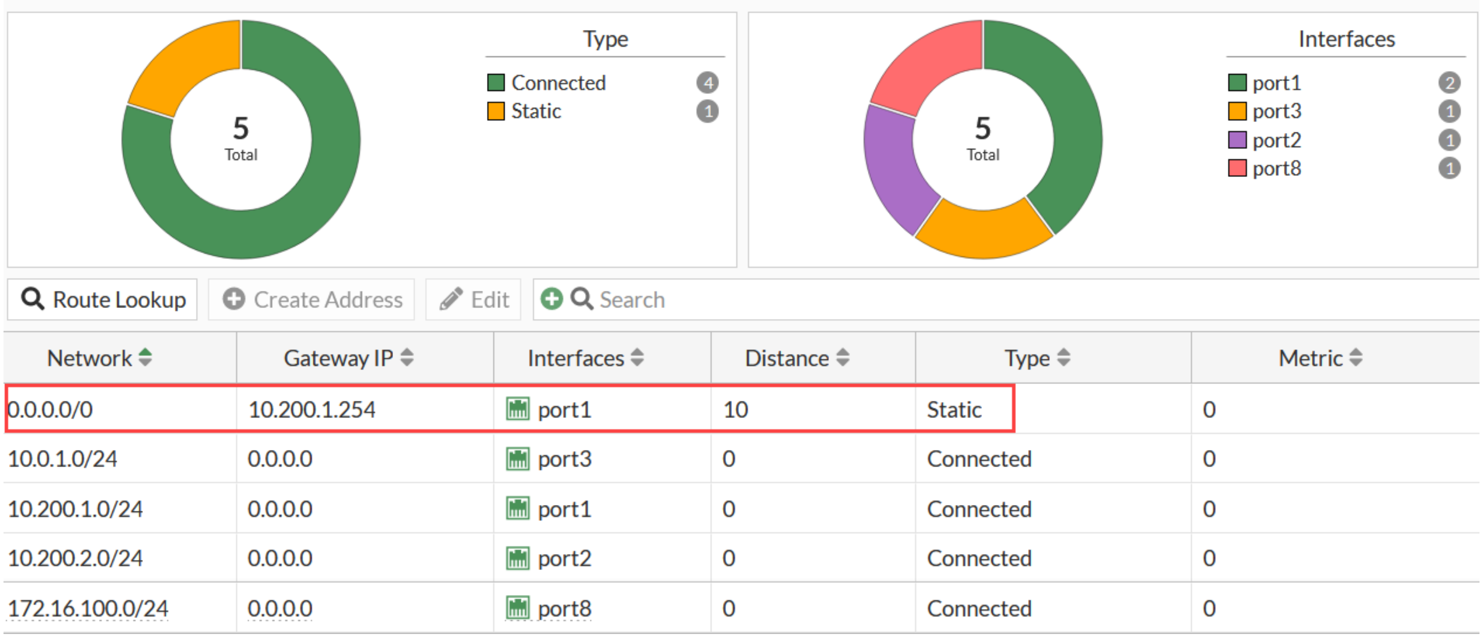
Before you begin the next exercise, you will restore the **port1** interface settings and bring it up, which will restore the port1 default route as the best route in the routing table.

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

3. Close the browser.

Exercise 2: Configuring Equal-Cost Multi Path Routing

Exercise 2: Configuring Equal-Cost Multi-Path Routing

In this exercise, you will configure equal-cost multi-path (ECMP) routing on Local-FortiGate to load balance the internet traffic between port1 and port2.

Configure Administrative Distance

To establish ECMP, first, you will configure multiple static routes with the same administrative distance.

> **Take the Expert Challenge!**
>
> On the Local-FortiGate GUI (admin/password), complete the following:
>
> - Change the **port2** static route **Administrative Distance** to **10**.
> - Verify that both **port1** and **port2** default routes are present in the routing table.
>
> If you require assistance, or to verify your work, use the step-by-step instructions that follow.

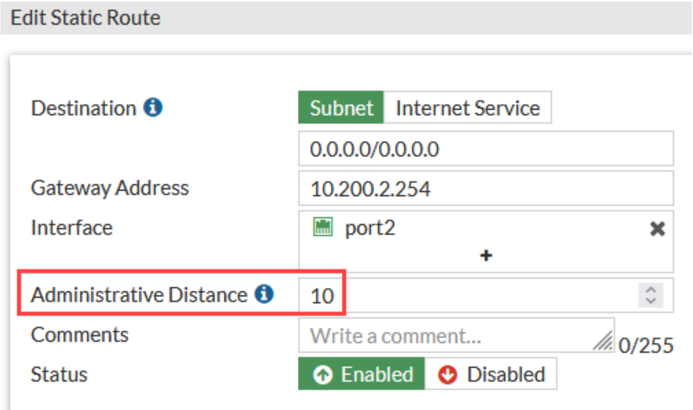
To configure administrative distance

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.

2. Click **Network** > **Static Routes**.

3. Double-click the **port2** static route to edit it.

4. In the **Administrative Distance** field, change the value to **10**.



Edit Static Route

Destination: Subnet | Internet Service
0.0.0.0/0.0.0.0

Gateway Address: 10.200.2.254

Interface: port2

Administrative Distance: 10

Comments: Write a comment... 0/255

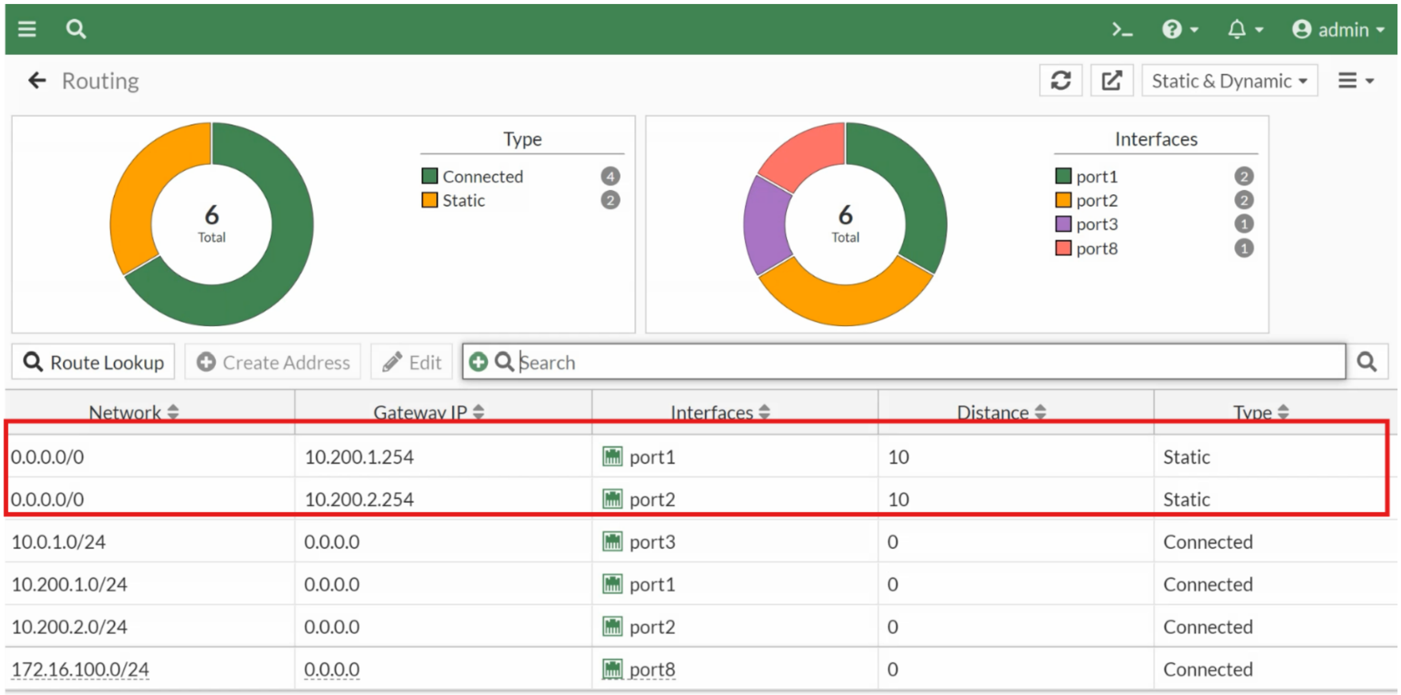
Status: Enabled | Disabled

5. 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. Verify that both default routes are installed in the routing table.



Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	10.200.1.254	port1	10	Static
0.0.0.0/0	10.200.2.254	port2	10	Static
10.0.1.0/24	0.0.0.0	port3	0	Connected
10.200.1.0/24	0.0.0.0	port1	0	Connected
10.200.2.0/24	0.0.0.0	port2	0	Connected
172.16.100.0/24	0.0.0.0	port8	0	Connected

Change the ECMP Load Balancing Algorithm

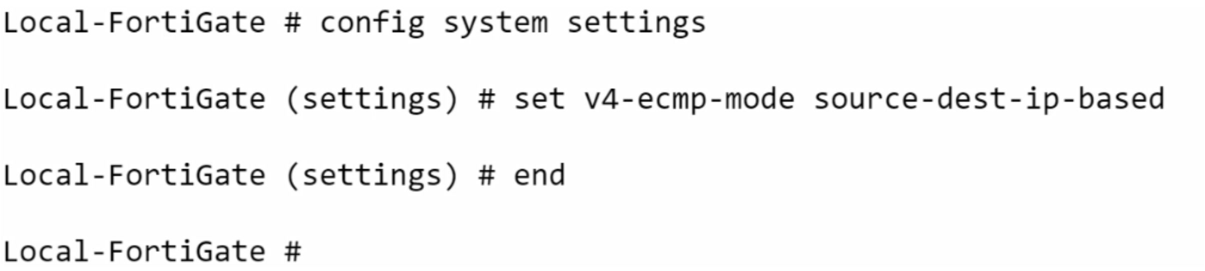
By default, the ECMP load balancing algorithm is based on **the source IP address**. This works well when there are multiple clients generating traffic. In the lab network, because you have only one client (the Local-Client VM), the source IP address method does not balance any traffic to the second route. FortiGate always uses only one route. For this reason, you will change the load balancing method to use both source and destination IP addresses. Using this method, as long as the traffic goes to multiple destination IP addresses, FortiGate load balances the traffic across both routes.

To modify the ECMP load balancing method

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.

2. Enter the following commands to change the ECMP load balancing method:

```
config system settings

set v4-ecmp-mode source-dest-ip-based

end
```



```
Local-FortiGate # config system settings

Local-FortiGate (settings) # set v4-ecmp-mode source-dest-ip-based

Local-FortiGate (settings) # end

Local-FortiGate #
```

3. Leave the Local-FortiGate CLI session open.

Verify Traffic Routing

You will generate some HTTP traffic and verify traffic routing using the **Forward Traffic** logs.

Take the Expert Challenge!

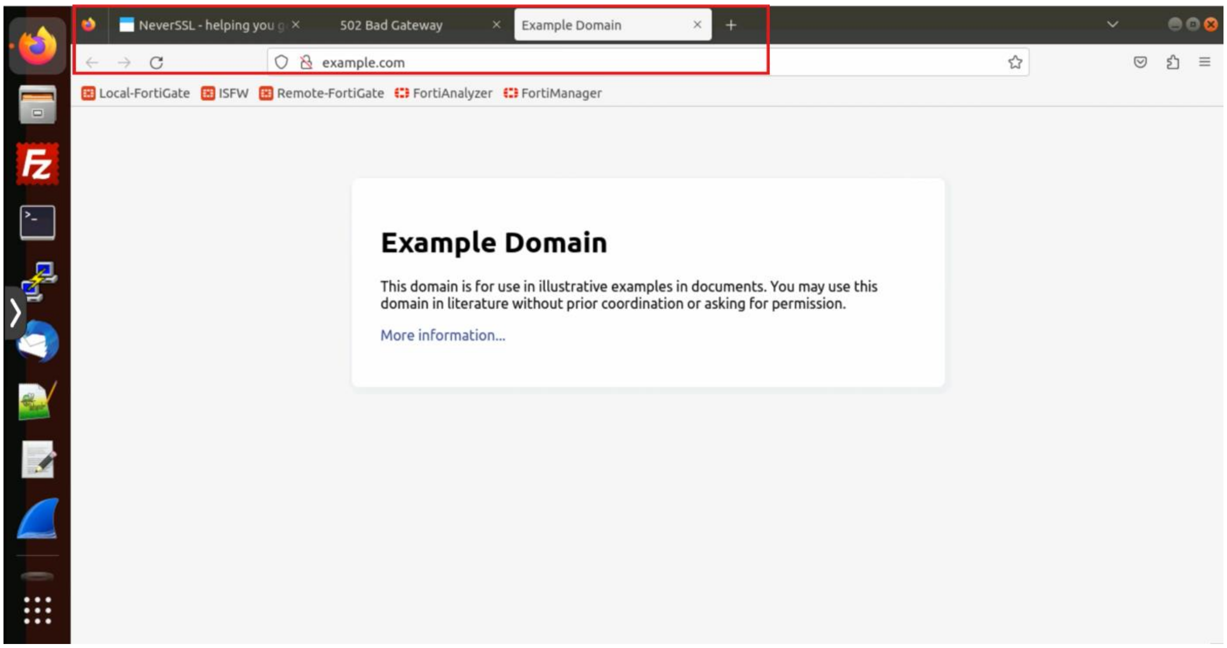
- On the Local-Client VM, open a few new browser tabs, and then generate some HTTP traffic.
- Verify the traffic routing on Local-FortiGate, using the **Forward Traffic** logs.
- Identify why all the outgoing packets are still being routed through **port1**.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

To verify traffic routing

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



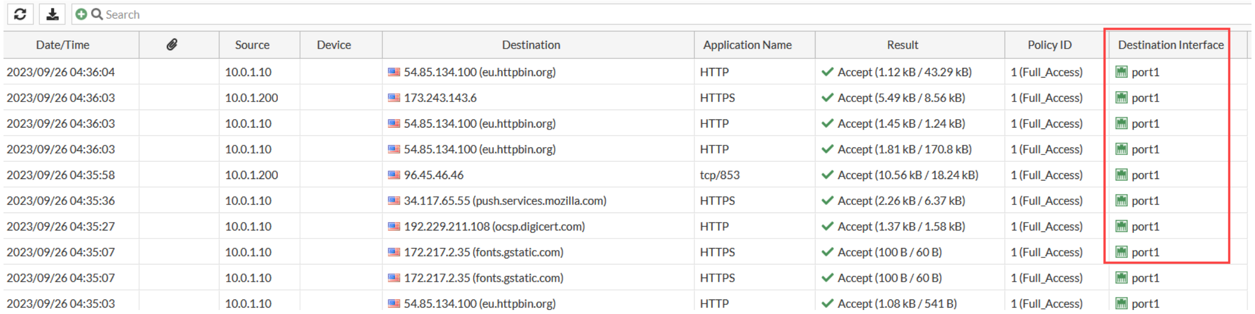
Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...

2. On the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.

3. In the relevant log entries for the websites you accessed, identify the **Destination Interface**.



Date/Time	📎	Source	Device	Destination	Application Name	Result	Policy ID	Destination Interface
2023/09/26 04:36:04		10.0.1.10		54.85.134.100 (eu.httpbin.org)	HTTP	✓ Accept (1.12 kB / 43.29 kB)	1 (Full_Access)	port1
2023/09/26 04:36:03		10.0.1.200		173.243.143.6	HTTPS	✓ Accept (5.49 kB / 8.56 kB)	1 (Full_Access)	port1
2023/09/26 04:36:03		10.0.1.10		54.85.134.100 (eu.httpbin.org)	HTTP	✓ Accept (1.45 kB / 1.24 kB)	1 (Full_Access)	port1
2023/09/26 04:36:03		10.0.1.10		54.85.134.100 (eu.httpbin.org)	HTTP	✓ Accept (1.81 kB / 170.8 kB)	1 (Full_Access)	port1
2023/09/26 04:35:58		10.0.1.200		96.45.46.46	tcp/853	✓ Accept (10.56 kB / 18.24 kB)	1 (Full_Access)	port1
2023/09/26 04:35:36		10.0.1.10		34.117.65.55 (push.services.mozilla.com)	HTTPS	✓ Accept (2.26 kB / 6.37 kB)	1 (Full_Access)	port1
2023/09/26 04:35:27		10.0.1.10		192.229.211.108 (ocsp.digicert.com)	HTTP	✓ Accept (1.37 kB / 1.58 kB)	1 (Full_Access)	port1
2023/09/26 04:35:07		10.0.1.10		172.217.2.35 (fonts.gstatic.com)	HTTPS	✓ Accept (100 B / 60 B)	1 (Full_Access)	port1
2023/09/26 04:35:07		10.0.1.10		172.217.2.35 (fonts.gstatic.com)	HTTPS	✓ Accept (100 B / 60 B)	1 (Full_Access)	port1
2023/09/26 04:35:03		10.0.1.10		54.85.134.100 (eu.httpbin.org)	HTTP	✓ Accept (1.08 kB / 541 B)	1 (Full_Access)	port1

Why are all the outgoing packets still being routed through port1????

Stop and think!

The **port2** route is not being used to route internet traffic. Why?

At the beginning of this exercise, you set a distance of 10 on the port2 route but you didn't change its priority. The port2 route priority is still 5, as you configured it in the previous exercise. In addition, the port1 route has distance and priority values of 10 and 1, respectively.

When two routes to the same destination have the same distance, both remain in the routing table. However, if the priorities are different, FortiGate uses the route with the lowest priority value—port1 in this case. To achieve ECMP with static routes, the distance and priority values must be the same for all routes.

Configure Priority

You will change the priority value for the **port2** route to match the **port1** route.

Take the Expert Challenge!

On the Local-FortiGate GUI, modify the static routing configuration so both default routes are eligible for ECMP.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

To configure priority

1. Continuing on the Local-FortiGate GUI, click **Network** > **Static Routes**.
2. Double-click the **port2** default route to edit it.
3. Click **+** to expand the **Advanced Options** section.
4. Change the **Priority** value to **1**.
5. Click **OK**.

Verify ECMP

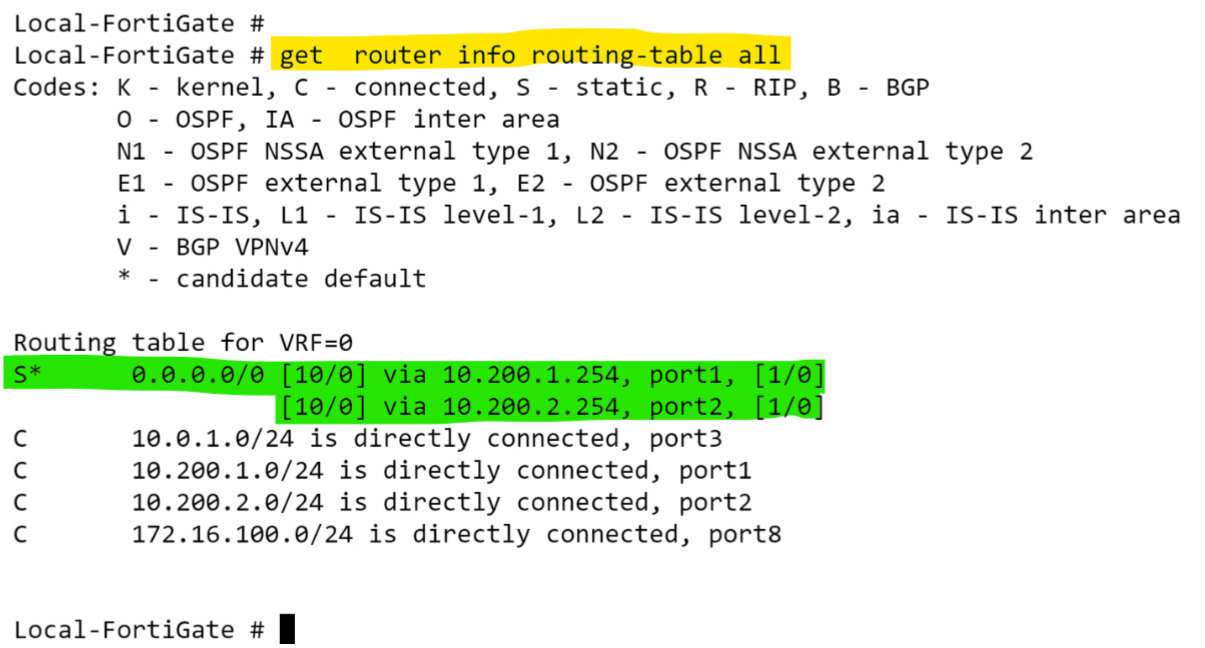
Now that both port1 and port2 routes share the same distance and priority values, they are eligible for ECMP. First, you will verify the routing table, and then you will verify traffic routing using the **Forward Traffic** logs.

To verify the routing table

1. Return to the Local-FortiGate CLI session, and then enter the following command on Local-FortiGate:

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

2. Verify that both default routes are currently active.



```
Local-FortiGate #
Local-FortiGate # get  router info routing-table all
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
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
                  [10/0] via 10.200.2.254, port2, [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


Local-FortiGate #
```

To configure the CLI sniffer

1. Continuing on the Local-FortiGate CLI session, enter the following command:

```
diagnose sniffer packet any 'not host 172.16.100.1 and not host 172.16.100.3
and tcp[13]&2==2 and port 80' 4
```

The filter 'tcp[13]&2==2' matches packets with the SYN flag on, so the output will show all SYN packets for port 80 (HTTP).

2. Leave the Local-FortiGate CLI window open in the background.

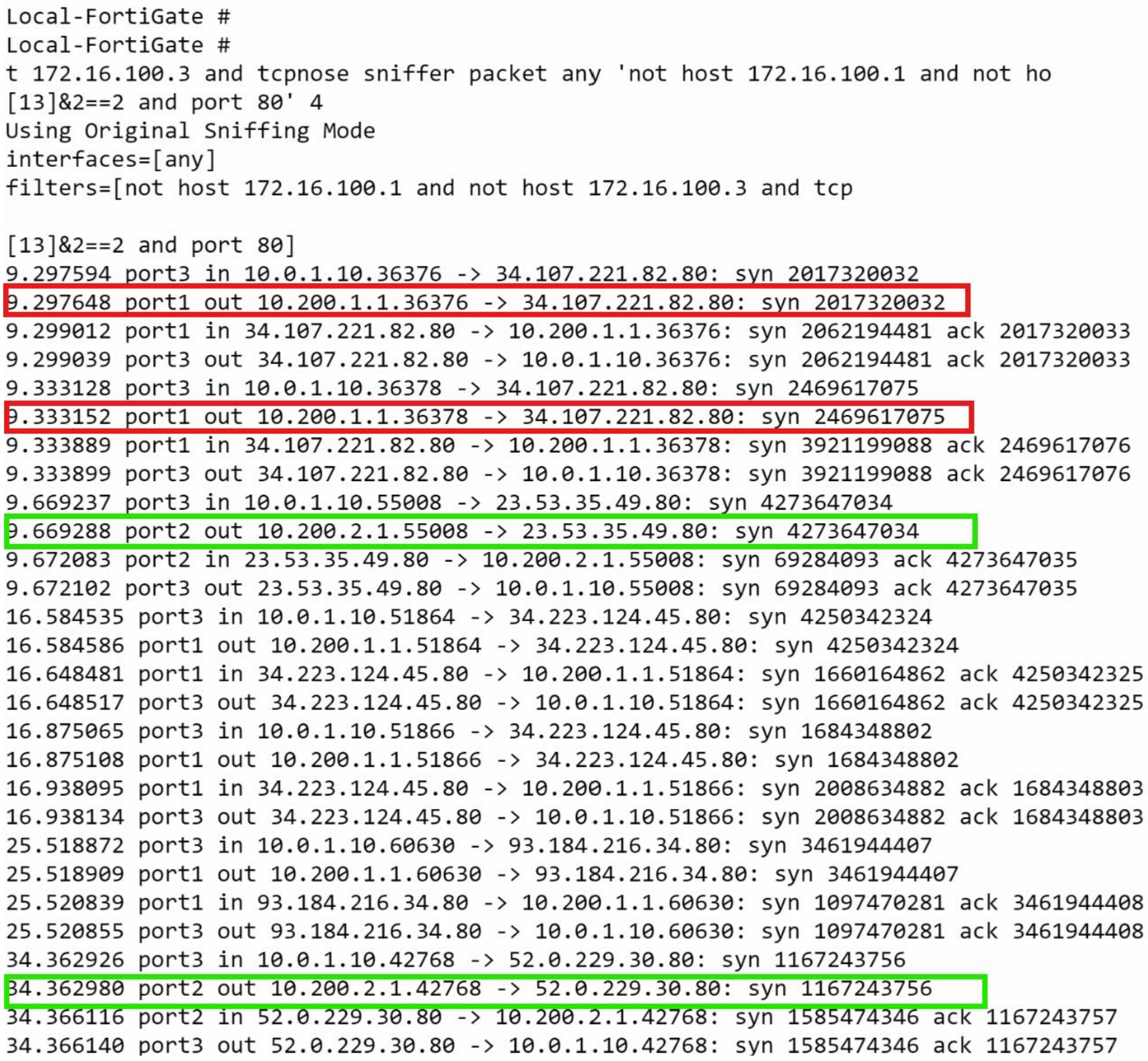
To verify ECMP routing

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

2. Return to the Local-FortiGate CLI session, and then press `Ctrl`+`C` to stop the sniffer.

3. Analyze the sniffer output.

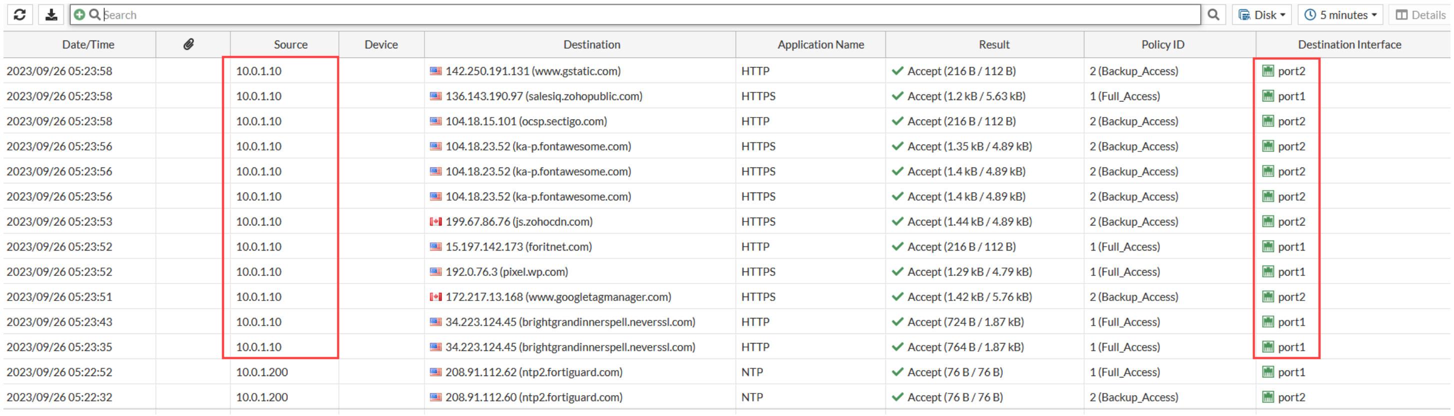


```
Local-FortiGate #
Local-FortiGate #
t 172.16.100.3 and tcpnose sniffer packet any 'not host 172.16.100.1 and not ho
[13]&2==2 and port 80' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[not host 172.16.100.1 and not host 172.16.100.3 and tcp

[13]&2==2 and port 80]
9.297594 port3 in 10.0.1.10.36376 -> 34.107.221.82.80: syn 2017320032
9.297648 port1 out 10.200.1.1.36376 -> 34.107.221.82.80: syn 2017320032
9.299012 port1 in 34.107.221.82.80 -> 10.200.1.1.36376: syn 2062194481 ack 2017320033
9.299039 port3 out 34.107.221.82.80 -> 10.0.1.10.36376: syn 2062194481 ack 2017320033
9.333128 port3 in 10.0.1.10.36378 -> 34.107.221.82.80: syn 2469617075
9.333152 port1 out 10.200.1.1.36378 -> 34.107.221.82.80: syn 2469617075
9.333889 port1 in 34.107.221.82.80 -> 10.200.1.1.36378: syn 3921199088 ack 2469617076
9.333899 port3 out 34.107.221.82.80 -> 10.0.1.10.36378: syn 3921199088 ack 2469617076
9.669237 port3 in 10.0.1.10.55008 -> 23.53.35.49.80: syn 4273647034
9.669288 port2 out 10.200.2.1.55008 -> 23.53.35.49.80: syn 4273647034
9.672083 port2 in 23.53.35.49.80 -> 10.200.2.1.55008: syn 69284093 ack 4273647035
9.672102 port3 out 23.53.35.49.80 -> 10.0.1.10.55008: syn 69284093 ack 4273647035
16.584535 port3 in 10.0.1.10.51864 -> 34.223.124.45.80: syn 4250342324
16.584586 port1 out 10.200.1.1.51864 -> 34.223.124.45.80: syn 4250342324
16.648481 port1 in 34.223.124.45.80 -> 10.200.1.1.51864: syn 1660164862 ack 4250342325
16.648517 port3 out 34.223.124.45.80 -> 10.0.1.10.51864: syn 1660164862 ack 4250342325
16.875065 port3 in 10.0.1.10.51866 -> 34.223.124.45.80: syn 1684348802
16.875108 port1 out 10.200.1.1.51866 -> 34.223.124.45.80: syn 1684348802
16.938095 port1 in 34.223.124.45.80 -> 10.200.1.1.51866: syn 2008634882 ack 1684348803
16.938134 port3 out 34.223.124.45.80 -> 10.0.1.10.51866: syn 2008634882 ack 1684348803
25.518872 port3 in 10.0.1.10.60630 -> 93.184.216.34.80: syn 3461944407
25.518909 port1 out 10.200.1.1.60630 -> 93.184.216.34.80: syn 3461944407
25.520839 port1 in 93.184.216.34.80 -> 10.200.1.1.60630: syn 1097470281 ack 3461944408
25.520855 port3 out 93.184.216.34.80 -> 10.0.1.10.60630: syn 1097470281 ack 3461944408
34.362926 port3 in 10.0.1.10.42768 -> 52.0.229.30.80: syn 1167243756
34.362980 port2 out 10.200.2.1.42768 -> 52.0.229.30.80: syn 1167243756
34.366116 port2 in 52.0.229.30.80 -> 10.200.2.1.42768: syn 1585474346 ack 1167243757
34.366140 port3 out 52.0.229.30.80 -> 10.0.1.10.42768: syn 1585474346 ack 1167243757
```

The SYN packets are egressing both `port1` and `port2`. This verifies that Local-FortiGate is now load balancing all internet traffic across both routes.

4. On the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.

5. Identify the **Destination Interface** in the relevant log entries for the websites you accessed.



Date/Time	🖇	Source	Device	Destination	Application Name	Result	Policy ID	Destination Interface
2023/09/26 05:23:58		10.0.1.10		142.250.191.131 (www.gstatic.com)	HTTP	✓ Accept (216 B / 112 B)	2 (Backup_Access)	port2
2023/09/26 05:23:58		10.0.1.10		136.143.190.97 (salesiq.zohopublic.com)	HTTPS	✓ Accept (1.2 kB / 5.63 kB)	1 (Full_Access)	port1
2023/09/26 05:23:58		10.0.1.10		104.18.15.101 (ocsp.sectigo.com)	HTTP	✓ Accept (216 B / 112 B)	2 (Backup_Access)	port2
2023/09/26 05:23:56		10.0.1.10		104.18.23.52 (ka-p.fontawesome.com)	HTTPS	✓ Accept (1.35 kB / 4.89 kB)	2 (Backup_Access)	port2
2023/09/26 05:23:56		10.0.1.10		104.18.23.52 (ka-p.fontawesome.com)	HTTPS	✓ Accept (1.4 kB / 4.89 kB)	2 (Backup_Access)	port2
2023/09/26 05:23:56		10.0.1.10		104.18.23.52 (ka-p.fontawesome.com)	HTTPS	✓ Accept (1.4 kB / 4.89 kB)	2 (Backup_Access)	port2
2023/09/26 05:23:53		10.0.1.10		199.67.86.76 (js.zohocdn.com)	HTTPS	✓ Accept (1.44 kB / 4.89 kB)	2 (Backup_Access)	port2
2023/09/26 05:23:52		10.0.1.10		15.197.142.173 (foritnet.com)	HTTP	✓ Accept (216 B / 112 B)	1 (Full_Access)	port1
2023/09/26 05:23:52		10.0.1.10		192.0.76.3 (pixel.wp.com)	HTTPS	✓ Accept (1.29 kB / 4.79 kB)	1 (Full_Access)	port1
2023/09/26 05:23:51		10.0.1.10		172.217.13.168 (www.googletagmanager.com)	HTTPS	✓ Accept (1.42 kB / 5.76 kB)	2 (Backup_Access)	port2
2023/09/26 05:23:43		10.0.1.10		34.223.124.45 (brightgrandinnerspell.neverssl.com)	HTTP	✓ Accept (724 B / 1.87 kB)	1 (Full_Access)	port1
2023/09/26 05:23:35		10.0.1.10		34.223.124.45 (brightgrandinnerspell.neverssl.com)	HTTP	✓ Accept (764 B / 1.87 kB)	1 (Full_Access)	port1
2023/09/26 05:22:52		10.0.1.200		208.91.112.62 (ntp2.fortiguard.com)	NTP	✓ Accept (76 B / 76 B)	1 (Full_Access)	port1
2023/09/26 05:22:32		10.0.1.200		208.91.112.60 (ntp2.fortiguard.com)	NTP	✓ Accept (76 B / 76 B)	2 (Backup_Access)	port2