



# FortiGate Route Preference and Priority

## Technical Note

<i>FortiGate Route Preference and Priority Technical Note</i>	
<b>Document Version:</b>	Version 1
<b>Publication Date:</b>	13 April 2005
<b>Description:</b>	This technical note explains how to configure the FortiGate unit to select a particular route when two or more static and/or dynamic routes to the same destination are present in the FortiGate routing table.
<b>Product:</b>	FortiGate v2.80 MR9
<b>Document Number:</b>	01-28009-0197-20050413

**Fortinet Inc.**

© Copyright 2005 Fortinet Inc. All rights reserved.

No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet Inc.

*FortiGate Route Preference and Priority Technical Note*

FortiGate v2.80 MR9

13 April 2005

01-28009-0197-20050413

Trademarks

Products mentioned in this document are trademarks or registered trademarks of their respective holders.

---

# Table of Contents

How the routing table is built .....	5
How routing decisions are made .....	5
How administrative distance affects route preference .....	6
How route sequence affects route priority .....	6
How adding static routes and route policies affect route selection .....	7
Preferences for routes associated with dynamic interfaces.....	8
Priority routing between static routes and routes associated with dynamic interfaces .....	9
Examples .....	9
Failover configuration using administrative distances.....	10
Forwarding packets through the preferred physical interface .....	11
Adjusting route sequence to create static route preference.....	12



This technical note explains how to configure the FortiGate unit to select a particular route when two or more static and/or dynamic routes to the same destination are present in the FortiGate routing table. The following sections are included:

- [How the routing table is built](#)
- [How routing decisions are made](#)
- [How administrative distance affects route preference](#)
- [How route sequence affects route priority](#)
- [How adding static routes and route policies affect route selection](#)
- [Preferences for routes associated with dynamic interfaces](#)
- [Priority routing between static routes and routes associated with dynamic interfaces](#)
- [Examples](#)

## How the routing table is built

In the factory default configuration, the FortiGate routing table contains a single static default route. You can add routing information to the routing table by defining additional static routes. The table may include several different routes to the same destination—the IP addresses of the next-hop router specified in those routes or the FortiGate interfaces associated with those routes may vary.

The FortiGate unit selects the “best” route for a packet by evaluating the information in the routing table. The best route to a destination is typically associated with the shortest distance between the FortiGate unit and the closest next-hop router. In some cases, the next best route may be selected if the best route is unavailable for some reason. The best routes are installed in the FortiGate forwarding table, which is a subset of the FortiGate routing table. Packets are forwarded according to the information in the forwarding table.

## How routing decisions are made

Whenever a packet arrives at one of the FortiGate unit's interfaces, the FortiGate unit determines whether the packet was received on a legitimate interface by doing a reverse lookup using the source IP address in the packet header. If the FortiGate unit cannot communicate with the computer at the source IP address through the interface on which the packet was received, the FortiGate unit drops the packet.

If the destination address can be matched to a local address (and the local configuration permits delivery), the FortiGate unit delivers the packet to the local network. If the packet is destined for another network, the FortiGate unit forwards the packet to a next-hop router according to a route policy and/or the information stored in the FortiGate forwarding table.

## How administrative distance affects route preference

When several entries to the same destination are present in the routing table, you can cause the FortiGate unit to select a primary (preferred) route by lowering the administrative distance associated with one of those routes.

All entries in the routing table are associated with an administrative distance. If the routing table contains several entries that point to the same destination (the entries may have different gateways or interface associations), the FortiGate unit compares the administrative distances of those entries, selects the entries having the lowest distances, and installs them as routes in the FortiGate forwarding table. As a result, the FortiGate forwarding table only contains routes having the lowest distances to every possible destination.










If needed, you can create a static route through the CLI and specify its sequence number to influence routing priority in the forwarding table. That is, routes to the same destination having lower administrative distances are considered preferable, and among preferred routes, routes having the lowest sequence numbers are selected first to route packets. For more information, see [“How route sequence affects route priority”](#) below.

## How route sequence affects route priority

After the FortiGate unit selects static routes for the forwarding table based on their administrative distances, the sequence numbers of those routes determines routing priority. When two routes to the same destination exist in the forwarding table, the route having the lowest sequence number is considered the highest priority route.

When you add a static route to the Static Route list through the web-based manager, the FortiGate unit assigns the next unassigned sequence number to the entry automatically. For example, in [Figure 1](#), two static routes to the same destination (1.1.1.0/24) were created to illustrate how entry numbers and sequence numbers are assigned through the web-based manager. The two routes specify the same gateway, but in one case, the packet would leave the FortiGate unit through the interface named “external”, and in the second case, the packet would leave the FortiGate unit through the interface named “dmz”.

Figure 1: Static routes created through web-based manger

Create New						
#	IP	Mask	Gateway	Device	Distance	
1	0.0.0.0	0.0.0.0	192.168.100.1	external	10	  
2	1.1.1.0	255.255.255.0	172.20.10.1	external	2	  
3	1.1.1.0	255.255.255.0	172.20.10.1	dmz	2	  

Because entry number 2 was created first and entry number 3 was created second, their sequence numbers in the routing table are 2 and 3 respectively. When the FortiGate unit evaluates these two routes to the same destination, both will be added to the forwarding table because they have low administrative distances. After a route has been added to the forwarding table, its sequence number determines the priority of the route. Because the second entry has the lowest sequence number, it is the preferred route.



**Note:** You can display the sequence numbers of static routes in the routing table through the CLI: type `config router static`, and then type `get`. The sequence number of a route is equivalent to the `edit <ID_integer>` value that one enters when defining a static route through the CLI. For more information, see `config router static` in the *FortiGate CLI Reference*.

The order of entries in the Static Route list typically mirrors the sequence of static routes in the routing table when all static routes are configured through the web-based manager. However, because you can specify the sequence number of a static route when you add the route through the CLI, the sequence number of a route may not always match its entry number in the Static Route list. Sequence numbers can be specified for static routes through the CLI only. The # column in the Static Route list simply displays how many static routes are present in the routing table.

In summary, if a route in the routing table has a low sequence number compared to a route to the same destination having a high sequence number, the FortiGate unit will choose the route with the low sequence number before choosing the route having a high sequence number. Because you can use the CLI to specify which sequence numbers to use when defining static routes, routes to the same destination can be prioritized according to their sequence numbers. To prioritize a static route, you must create the route using the `config router static` CLI command and specify a low sequence number for the route.

## How adding static routes and route policies affect route selection

When you add a static route to the FortiGate configuration, the FortiGate unit evaluates the information to determine if it represents a different route compared to any other route already present in the FortiGate routing table. If no route having the same destination exists in the routing table, the FortiGate unit adds the route to the routing table.

When route policies exist and a packet arrives at the FortiGate unit, the FortiGate unit starts at the top of the Policy Route list and attempts to match the packet with a policy. If a match is found and the policy contains enough information to route the packet (the IP address of the next-hop router must be specified as well as the FortiGate interface for forwarding packets to the next-hop router), the FortiGate unit routes the packet using the information in the policy. If no route policy matches the packet, the FortiGate unit routes the packet using the routing table.



**Note:** Because most policy settings are optional, a matching policy alone might not provide enough information for the FortiGate unit to forward the packet. The FortiGate unit may refer to the routing table in an attempt to match the information in the packet header with a route in the routing table.

For example, if the outgoing interface is the only item given in the policy, the FortiGate unit looks up the IP address of the next-hop router in the routing table. This situation could happen when the FortiGate interfaces are dynamic (the interface receives an IP address through DHCP or PPPoE) and you do not want or are unable to specify the IP address of the next-hop router because the IP address changes dynamically.

## Preferences for routes associated with dynamic interfaces

Routes associated with dynamic interfaces do not have sequence numbers. The FortiGate unit uses the index number of the route's associated physical interface to select the best route instead. When two routes associated with dynamic interfaces are present in the routing table and those routes point to the same destination, you cannot influence route priority through sequence numbers. However, you can view the physical-interface index numbers associated with those routes to determine which interface is preferred. When you know which interface is preferred, you can reconnect the physical interfaces if required to ensure that traffic is being forwarded through the interface having the lowest index number.

Each FortiGate physical interface has an index number that can be displayed using the `diag net interface list` CLI command. For example, the FortiGate-100 in the following example has three physical interfaces named `dmz`, `external`, and `internal` (your FortiGate unit may have different interface names). The output strings have been truncated for brevity:

```
Fortigate-100: # diag net interface list
if=lo family=00 type=772 index=1 ...
if=dmz family=00 type=1 index=2 ...
if=external family=00 type=1 index=3 ...
if=internal family=00 type=1 index=4 ...
```

The preferred physical interface has the lowest index number. In this example, the preferred physical interface is `dmz`, which has index number 2. The `external` interface is the next preferred physical interface. If both of these interfaces were dynamic and the routing table contained two routes to the same destination through these two interfaces, the FortiGate unit would select the route associated with the `dmz` interface and install that route in the forwarding table.



Index numbers cannot be changed. However, you can switch physical connections if required to force packets through the preferred interface (see [“Forwarding packets through the preferred physical interface” on page 11](#)). If your ISP assigns an IP address to the FortiGate interface through DHCP, simply unplug and reconnect the cable to the preferred interface. If your ISP assigns an IP address to the FortiGate interface through PPPoE, you will have to reconnect the cable to the preferred interface and then reconfigure the PPPoE settings for the interface (go to **System > Network > Interface** in the web-based manager, or use the `system network interface` CLI command to reconfigure the PPPoE settings).

## Priority routing between static routes and routes associated with dynamic interfaces

When the FortiGate routing table contains two routes to the same destination, but one route is a static route and the other is associated with a dynamic interface, the FortiGate unit will (by default) prefer the route associated with the dynamic interface. By default, static routes have an administrative distance of 10 (the distance to the next-hop router), and routes associated with dynamic interfaces have an administrative distance of 1 (the distance to the default gateway retrieved from the DHCP or PPPoE server). Thus, unless you modify the default distance settings, a route learned through DHCP or PPPoE will be preferred compared to a static route.

To change the administrative distance associated with a dynamic interface:

- In the web-based manager, go to **System > Network > Interface** and enter a different value in the Distance field under Addressing mode.
- Using the CLI, type `config system interface` and modify the `distance` attribute associated with the DHCP or PPPoE interface.

If you want to force the FortiGate unit to prefer a route through a static interface instead of a route through a dynamic interface, you can edit the sequence number of the static route so that the number is lower than the index number of the dynamic interface. For more information, see [“Adjusting route sequence to create static route preference” on page 12](#).

## Examples

A number of examples are included in this section to demonstrate how to configure static routes, swap physical connections, and adjust static route sequence numbers to influence preferred routes and route priority:

- [Failover configuration using administrative distances](#)
- [Forwarding packets through the preferred physical interface](#)
- [Adjusting route sequence to create static route preference](#)

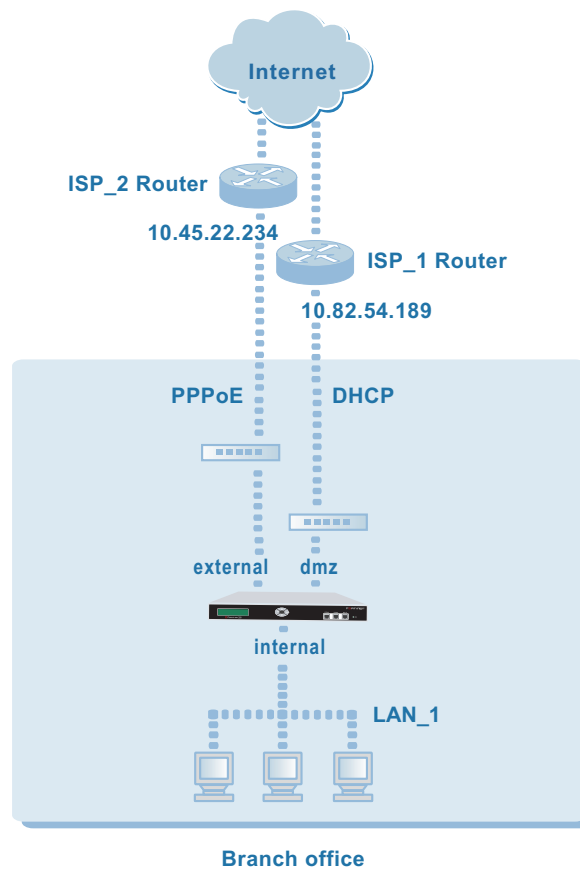


**Note:** In the following example configurations, private IP addresses are used for both private and public IP addresses.

## Failover configuration using administrative distances

A typical failover scenario usually involves the FortiGate unit having two different physical interfaces to the Internet (see the example configuration in [Figure 2](#)). In this type of configuration, one of the connections (for example, the dmz interface) acts as the primary link to the Internet, and the other connection (for example, the external interface) is not used unless the primary link goes down. A ping server must be configured on the primary interface. The ping server detects link failure and automatically initiates switchover to the failover route.

**Figure 2: Example failover configuration**



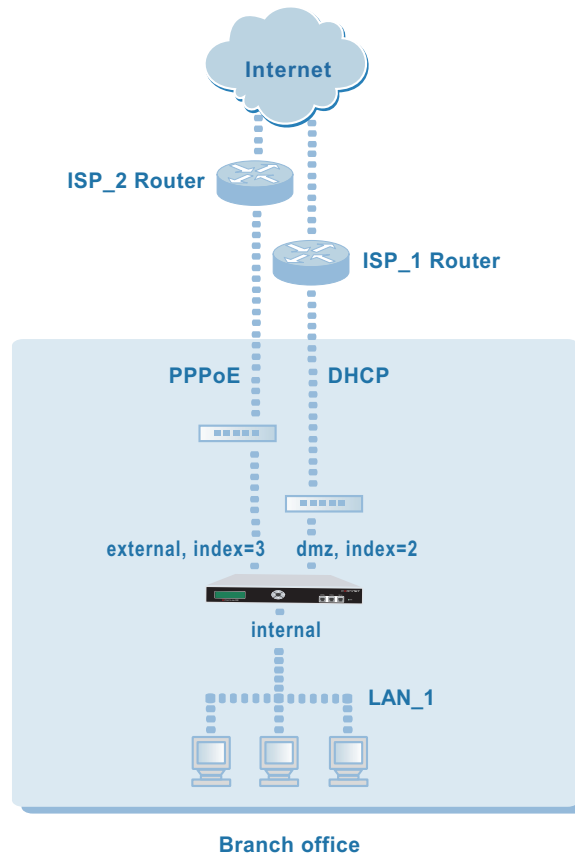
To configure this type of failover scenario, the following general configuration steps must be performed at the FortiGate unit:

- Edit the default route to make the ISP\_1 Router interface (for example, 10.82.54.189) the default gateway for the FortiGate unit. When you edit the settings, change the Distance value to a low number (for example, 1).
- Add a static route that points to the ISP\_2 Router interface (for example, 10.45.22.234). Keep the default administrative distance value of 10.
- Configure a ping server on the FortiGate primary interface to the Internet. In [Figure 2](#), the interface name is dmz. The name of the interface on your FortiGate unit may be different.

## Forwarding packets through the preferred physical interface

This example demonstrates routing behavior when two routes learned through the DHCP and PPPoE protocols have the same administrative distance but different priorities. In the example failover configuration shown in [Figure 3](#), the FortiGate external and dmz interfaces are dynamic, and the routes associated with those interfaces both have the same administrative distance (a value of 1 by default).

**Figure 3: Example physical interface index number configuration**



When both routes are available, the FortiGate unit looks up the index number of each physical interface to determine which route is preferred. The FortiGate unit will always select the route associated with the dmz interface because the index number of the dmz interface is lowest—if the route associated with the dmz interface were to become unavailable, the FortiGate unit would forward traffic through the external interface instead.



**Note:** The index numbers assigned to FortiGate interfaces may vary from one FortiGate model to the next. For example, the interfaces of all FortiGate-100 units have the same index numbers (2 for the dmz interface, 3 for the external interface, and 4 for the internal interface), but the index numbers assigned to a FortiGate-300 or a FortiGate-4000 may be different.

If you wanted to force the FortiGate unit to select the route through the external interface instead of the route through the dmz interface (when both routes are available) and configure failover to ISP\_1 Router if ISP\_2 Router were to become unavailable, you would need to:

- Reconnect the ISP\_2 Router interface to the dmz interface and add PPPoE settings to the dmz interface. Leave the distance attribute set to 1.
- Reconnect the ISP\_1 Router interface to the external interface and select the DHCP addressing option for the interface. Leave the distance attribute set to 1.

When both distances are the same, both routes are installed in the forwarding table.



**Note:** If you wanted only one of the routes to be installed, you would increase the Distance value of the route to ignore—the route having the lowest distance would be installed in the forwarding table.

- Delete all static routes that reference the dmz and external interfaces, including the default static route. The FortiGate unit will learn its routes through DHCP and PPPoE dynamically.
- Configure a ping server on both interfaces. Afterward, when one of the routes becomes temporarily unavailable (due to a dynamic IP address change), the ping server will detect the change and the associated route will be removed from the routing table automatically. When the FortiGate unit receives a new IP address for the dynamic interface, the FortiGate unit will add the route to the ISP's next-hop router to the FortiGate routing table.

## Adjusting route sequence to create static route preference

In the following example, the FortiGate routing table contains two routes to the same destination. The dmz interface has a static IP address, and the external interface receives an IP address dynamically. In the example, the output strings have been truncated for brevity:

```
Fortigate-500: # diag net interface list

if=lo family=00 type=772 index=1 ...

if=dmz family=00 type=1 index=2 ...

if=external family=00 type=1 index=3 ...

if=internal family=00 type=1 index=4 ...
```

By default, the FortiGate unit prefers the route through the dynamic interface because that route has a lower administrative distance. To cause the FortiGate unit to prefer the route through the dmz (static) interface instead, the sequence number of the static route (for example, 4) must be decreased so that the sequence number is lower than the index number of the external interface.

To display the sequence number of the static route, type `show router static`:

```
Fortigate-500 # show router static
config router static
  edit 4
    set device "dmz"
    set gateway 10.100.0.148
  next
end
```

The sequence number of the static route (4) must be changed as follows so that the sequence number is lower than the index value of the external interface (3).

```
Fortigate-500 # config router static
(static)# delete 4

(static)# edit 2
new entry '2' added

(40)# set device dmz

(40)# set gateway 10.100.0.148

(static)# end

Fortigate-500 # show router static
config router static
  edit 2
    set device "dmz"
    set gateway 10.100.0.148
  next
end
```

Because the sequence number of the static route has been changed to 2 (a value that is lower than the index number of the route associated with the dynamic interface), the static route is now the preferred route.



**Caution:** Adding static routes through the web-based manager has the potential to reset the preferred route. Remember, when you add a static route through the web-based manager, the FortiGate unit assigns the next unassigned sequence number to the route automatically. If the automatically assigned sequence number is lower than the sequence number of existing static routes and/or lower than the index number of the dynamic interface, the FortiGate unit may prefer the new static route.

