



Routing

The system uses a routing table to determine the egress interface for packets entering the system. The following topics explain routing basics and how to configure routing on the device.

- [Routing Overview, on page 1](#)
- [Configuring Static Routes, on page 3](#)
- [Monitoring Routing, on page 4](#)

Routing Overview

The following topics describe how routing behaves within the FTD device. Routing is the act of moving information across a network from a source to a destination. Along the way, at least one intermediate node is typically encountered. Routing involves two basic activities: determining optimal routing paths and transporting packets through a network.

How NAT Affects Route Selection

FTD uses both routing table and Network Address Translations (NAT) XLATE (translation) tables for routing decisions. To handle destination IP translated traffic, that is, untranslated traffic, the system searches for an existing XLATE or a static translation to select the egress interface.

The selection process follows these steps:

1. If a destination IP translating XLATE already exists, the egress interface for the packet is determined from the XLATE table, but not from the routing table.
2. If a destination IP translating XLATE does not exist, but a matching static NAT translation exists, then the egress interface is determined from the static NAT rule and an XLATE is created, and the routing table is not used.
3. If a destination IP translating XLATE does not exist and no matching static translation exists, the packet is not destination IP translated. The system processes this packet by looking up the route to select the egress interface, then source IP translation is performed (if necessary).

For regular dynamic outbound NAT, initial outgoing packets are routed using the route table and then the XLATE is created. Incoming return packets are forwarded using the existing XLATE only. For static NAT, destination translated incoming packets are always forwarded using an existing XLATE or static translation rules.

After selecting the egress interface, an additional route lookup is performed to find out suitable next hop that belongs to the selected egress interface. If there are no routes in the routing table that explicitly belong to a selected interface, the packet is dropped with a level 6 diagnostic syslog message 110001 generated (no route to host), even if there is another route for a given destination network that belongs to a different egress interface. If the route that belongs to a selected egress interface is found, the packet is forwarded to the corresponding next hop.

The Routing Table and Route Selection

When NAT XLATEs and rules do not determine the egress interface, the system uses the routing table to determine the path for a packet.

Routes in the routing table include a metric called “administrative distance” that provides a relative priority to a given route. If a packet matches more than one route entry, the one with the lowest distance is used. Directly connected networks (those defined on an interface) have the distance 0, so they are always preferred. Static routes have a default distance of 1, but you can create them with any distance between 1-254.

Routes that identify a specific destination take precedence over the default route (the route whose destination is 0.0.0.0/0).

How Forwarding Decisions Are Made

Forwarding decisions are made as follows:

- If the destination does not match an entry in the routing table, the packet is forwarded through the interface specified for the default route. If a default route has not been configured, the packet is discarded.
- If the destination matches a single entry in the routing table, the packet is forwarded through the interface associated with that route.
- If the destination matches more than one entry in the routing table, then the packet is forwarded out of the interface associated with the route that has the longer network prefix length.

For example, a packet destined for 192.168.32.1 arrives on an interface with the following routes in the routing table:

- 192.168.32.0/24 gateway 10.1.1.2
- 192.168.32.0/19 gateway 10.1.1.3

In this case, a packet destined to 192.168.32.1 is directed toward 10.1.1.2, because 192.168.32.1 falls within the 192.168.32.0/24 network. It also falls within the other route in the routing table, but 192.168.32.0/24 has the longest prefix within the routing table (24 bits verses 19 bits). Longer prefixes are always preferred over shorter ones when forwarding a packet.



Note

Existing connections continue to use their established interfaces even if a new similar connection would result in different behavior due to a change in routes.

Configuring Static Routes

Define static routes to tell the system where to send packets that are not bound for networks that are directly connected to the interfaces on the system.

You need at least one static route, the default route, for network 0.0.0.0/0. This route defines where to send packets whose egress interface cannot be determined by existing NAT xlates (translations) or static NAT rules, or other static routes.

You might need other static routes if the default gateway cannot be used to get to all networks. For example, the default route is usually an upstream router on the outside interface. If there are additional inside networks that are not directly connected to the device, and they cannot be accessed through the default gateway, you need static routes for each of those inside networks.

You cannot define static routes for the networks that are directly connected to system interfaces. The system automatically creates these routes.

Procedure

Step 1 Click **Device**, then click the link in the **Routing** summary.

Step 2 On the **Static Routing** page, do one of the following:

- To add a new route, click + > **Add Static Route**.
- Click the edit icon (✎) for the route you want to edit.

If you no longer need a route, click the trash can icon for the route to delete it.

Step 3 Configure the route properties

Protocol

Select whether the route is for an **IPv4** or **IPv6** address.

Gateway

Select the host network object that identifies the IP address for the gateway. Traffic is sent to this address.

Interface

Select the interface through which you want to send traffic. The gateway address needs to be accessible through this interface.

For bridge groups, you configure the route for the bridge group interface (BVI), not for the member interfaces.

Metric

The administrative distance for the route, between 1 and 254. The default is for static routes is 1. If there are additional routers between the interface and the gateway, enter the number of hops as the administrative distance.

Administrative distance is a parameter used to compare routes. The lower the number, the higher precedence the route is given. Connected routes (networks directly connected to an interface on the device) always take precedence over static routes.

Network

Select the network objects that identify the destination networks or hosts that should use the gateway in this route.

To define a default route, use the pre-defined any-ipv4 or any-ipv6 network objects, or create an object for the 0.0.0.0/0 (IPv4) or ::/0 (IPv6) network.

Step 4 Click OK.

Monitoring Routing

To monitor and troubleshoot routing, log into the device CLI and use the following commands.

- **show route** displays the routing table for the data interfaces, including routes for directly-connected networks.
- **show ipv6 route** displays the IPv6 routing table for the data interfaces, including routes for directly-connected networks.
- **show network** displays the configuration for the virtual management interface, including the management gateway. Routing through the virtual interface is not handled by the data interface routing table, unless you specify data-interfaces as the management gateway.
- **show network-static-routes** displays static routes configured for the virtual management interface using the **configure network static-routes** command. Normally, there will not be any static routes, as the management gateway suffices for management routing in most cases. These routes are not available to traffic on the data interfaces. This command is not available in the CLI console.