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
- Static Routes, on page 3
- Monitoring Routing, on page 6

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.

The Routing Table and Route Selection

When NAT translations (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 or ::/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.

Routing Table for Management Traffic

As a standard security practice, it is often necessary to segregate and isolate Management traffic from data traffic. To achieve this isolation, the FTD uses a separate routing table for management-only traffic vs. data traffic. Separate routing tables means that you can create separate default routes for data and management as well.

Through-the-device traffic always uses the data routing table.

From-the-device traffic, depending on the type, uses either the management routing table or the data routing table by default. If a match is not found in the default routing table, it checks the other routing table.

Management table from-the-device traffic includes features that open a remote file using HTTP, SCP, TFTP, and so on.

Data table from-the-device traffic includes all other features like ping, DNS, DHCP, and so on.

If you need from-the-box traffic to go out an interface that isn't in its default routing table, then you might need to specify that interface when you configure it, rather than relying on the fall back to the other table. The FTD checks the correct routing table for routes for that interface. For example, if you need a ping to go out a management-only interface, then specify the interface in the ping function. Otherwise, if there is a default route in the data routing table, then it will match the default route and never fall back to the management routing table.

The management routing table supports dynamic routing separate from the data interface routing table. A given dynamic routing process must run on either the management-only interface or the data interface; you cannot mix both types.

Management-only interfaces include any Management x/x (named "diagnostic") interfaces as well as any interfaces that you have configured to be management-only.

Note This routing table does not affect the special FTD Management logical interface that it uses to communicate with the FMC; that interface has its own routing table. The Diagnostic logical interface, on the other hand, uses the management-only routing table described in this section.

Note This routing table does not affect the special FTD Management virtual interface that it uses to communicate with the licensing server or for database updates; that interface has its own routing table. The Diagnostic physical interface, on the other hand, uses the management-only routing table described in this section.

Equal-Cost Multi-Path (ECMP) Routing

The Firepower Threat Defense device supports Equal-Cost Multi-Path (ECMP) routing.

You can have up to 3 equal cost static or dynamic routes per interface. For example, you can configure multiple default routes on the outside interface that specify different gateways.

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

In this case, traffic is load-balanced on the outside interface between 10.1.1.2, 10.1.1.3, and 10.1.1.4. Traffic is distributed among the specified gateways based on an algorithm that hashes the source and destination IP addresses, incoming interface, protocol, source and destination ports.

ECMP is not supported across multiple interfaces, so you cannot define a route to the same destination on a different interface. The following route is disallowed when configured with any of the routes above:

```
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.1
```

Static Routes

You can create static routes to provide basic routing for your network.

About Static and Default Routes

To route traffic to a non-connected host or network, you must define a route to the host or network, either using static or dynamic routing. Generally, you must configure at least one static route: a default route for all traffic that is not routed by other means to a default network gateway, typically the next hop router.

Default Route

The simplest option is to configure a default static route to send all traffic to an upstream router, relying on the router to route the traffic for you. A default route identifies the gateway IP address to which the FTD device sends all IP packets for which it does not have a learned or static route. A default static route is simply a static route with 0.0.0.0/0 (IPv4) or ::/0 (IPv6) as the destination IP address.

You should always define a default route.

Because the FTD uses separate routing tables for data traffic and for management traffic, you can optionally configure a default route for data traffic and another default route for management traffic. Note that from-the-device traffic uses either the management or data routing table by default depending on the type (see Routing Table for Management Traffic, on page 2), but will fall back to the other routing table if a route is not found. Default routes will always match traffic, and will prevent a fall back to the other routing table. In this case, you must specify the interface you want to use for egress traffic if that interface is not in the default routing table.

Static Routes

You might want to use static routes in the following cases:

- Your networks use an unsupported router discovery protocol.
- Your network is small and you can easily manage static routes.
- You do not want the traffic or CPU overhead associated with routing protocols.
- In some cases, a default route is not enough. The default gateway might not be able to reach the destination network, so you must also configure more specific static routes. For example, if the default gateway is outside, then the default route cannot direct traffic to any inside networks that are not directly connected to the FTD device.
- You are using a feature that does not support dynamic routing protocols.

Guidelines for Static Routing

Bridge Groups

- In routed mode, you must specify the BVI as the gateway; you cannot specify the member interface.
- For traffic that originates on the Firepower Threat Defense device (such as syslog or SNMP) that is destined through a bridge group member interface for a non-directly connected network, you need to configure either a default route or static routes so the Firepower Threat Defense device knows out of which bridge group member interface to send traffic. If you have servers that cannot all be reached through a single default route, then you must configure static 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 +.
- 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

Name

A display name for the route.

Description

An optional description of the purpose for the route.

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.

Protocol

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

Networks

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.

Gateway

Select the host network object that identifies the IP address for the gateway. Traffic is sent to this address. You cannot use the same gateway for routes on more than one interface.

Metric

The administrative distance for the route, between 1 and 254. The default 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.

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.