Static and Default Routes for Firepower Threat Defense

This chapter describes how to configure static and default routes on the FTD.

- About Static and Default Routes, on page 1
- Guidelines for Static and Default Routes, on page 3
- Add a Static Route, on page 3

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.

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.

**Route to null0 Interface to “Black Hole” Unwanted Traffic**

Access rules let you filter packets based on the information contained in their headers. A static route to the null0 interface is a complementary solution to access rules. You can use a null0 route to forward unwanted or undesirable traffic into a “black hole” so the traffic is dropped.

Static null0 routes have a favorable performance profile. You can also use static null0 routes to prevent routing loops. BGP can leverage the static null0 route for Remotely Triggered Black Hole routing.

**Route Priorities**

- Routes that identify a specific destination take precedence over the default route.
- When multiple routes exist to the same destination (either static or dynamic), then the administrative distance for the route determines priority. Static routes are set to 1, so they typically are the highest priority routes.
- When you have multiple static routes to the same destination with the same administrative distance, see Equal-Cost Multi-Path (ECMP) Routing.
- For traffic emerging from a tunnel with the Tunneled option, this route overrides any other configured or learned default routes.

**Transparent Firewall Mode and Bridge Group Routes**

For traffic that originates on the Firepower Threat Defense device and 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. Traffic that originates on the Firepower Threat Defense device might include communications to a syslog server or SNMP server. If you have servers that cannot all be reached through a single default route, then you must configure static routes. For transparent mode, you cannot specify the BVI as the gateway interface; only member interfaces can be used. For bridge groups in routed mode, you must specify the BVI in a static route; you cannot specify a member interface. See MAC Address vs. Route Lookups for more information.

**Static Route Tracking**

One of the problems with static routes is that there is no inherent mechanism for determining if the route is up or down. They remain in the routing table even if the next hop gateway becomes unavailable. Static routes are only removed from the routing table if the associated interface on the Firepower Threat Defense device goes down.

The static route tracking feature provides a method for tracking the availability of a static route and installing a backup route if the primary route should fail. For example, you can define a default route to an ISP gateway and a backup default route to a secondary ISP in case the primary ISP becomes unavailable.

The Firepower Threat Defense device implements static route tracking by associating a static route with a monitoring target host on the destination network that the Firepower Threat Defense device monitors using...
ICMP echo requests. If an echo reply is not received within a specified time period, the host is considered down, and the associated route is removed from the routing table. An untracked backup route with a higher metric is used in place of the removed route.

When selecting a monitoring target, you need to make sure that it can respond to ICMP echo requests. The target can be any network object that you choose, but you should consider using the following:

- The ISP gateway (for dual ISP support) address
- The next hop gateway address (if you are concerned about the availability of the gateway)
- A server on the target network, such as a syslog server, that the Firepower Threat Defense device needs to communicate with
- A persistent network object on the destination network

_A PC that may be shut down at night is not a good choice._

You can configure static route tracking for statically defined routes or default routes obtained through DHCP or PPPoE. You can only enable PPPoE clients on multiple interfaces with route tracking configured.

**Guidelines for Static and Default Routes**

**Firewall Mode and Bridge Groups**

- In transparent mode, static routes must use the bridge group member interface as the gateway; you cannot specify the BVI.
- In routed mode, you must specify the BVI as the gateway; you cannot specify the member interface.
- Static route tracking is not supported for bridge group member interfaces or on the BVI.

**IPv6**

- Static route tracking is not supported for IPv6.

**Clustering**

In clustering, static route monitoring is only supported on the primary unit.

**Add a Static Route**

A static route defines where to send traffic for specific destination networks. You should at a minimum define a default route. A default route is simply a static route with 0.0.0.0/0 as the destination IP address.
Procedure

Step 1  Choose Devices > Device Management, and edit the FTD device.
Step 2  Click the Routing tab.
Step 3  Select Static Route from the table of contents.
Step 4  Click Add Routes.
Step 5  Click the IPv4 or IPv6 radio button depending on the type of static route that you are adding.
Step 6  Choose the Interface to which this static route applies.
        For transparent mode, choose a bridge group member interface name. For routed mode with bridge groups,
        you can choose either the bridge group member interface for the BVI name. To “black hole” unwanted traffic,
        choose the Null0 interface.
Step 7  In the Available Network list, choose the destination network.
        To define a default route, create an object with the address 0.0.0.0/0 and select it here.
Step 8  In the Gateway or IPv6 Gateway field, enter or choose the gateway router which is the next hop for this
        route. You can provide an IP address or a Networks/Hosts object.
Step 9  In the Metric field, enter the number of hops to the destination network. Valid values range from 1 to 255;
        the default value is 1. The metric is a measurement of the “expense” of a route, based on the number of hops
        (hop count) to the network on which a specific host resides. Hop count is the number of networks that a
        network packet must traverse, including the destination network, before it reaches its final destination. The
        metric is used to compare routes among different routing protocols. The default administrative distance for
        static routes is 1, giving it precedence over routes discovered by dynamic routing protocols but not directly
        connected routes. The default administrative distance for routes discovered by OSPF is 110. If a static route
        has the same administrative distance as a dynamic route, the static route takes precedence. Connected routes
        always take precedence over static or dynamically discovered routes.
Step 10 (Optional) For a default route, click the Tunneled checkbox to define a separate default route for VPN traffic.
        You can define a separate default route for VPN traffic if you want your VPN traffic to use a different default
        route than your non VPN traffic. For example, traffic incoming from VPN connections can be easily directed
        towards internal networks, while traffic from internal networks can be directed towards the outside. When
        you create a default route with the tunneled option, all traffic from a tunnel terminating on the device that
        cannot be routed using learned or static routes, is sent to this route. You can configure only one default tunneled
        gateway per device. ECMP for tunneled traffic is not supported.
Step 11 (IPv4 static route only) To monitor route availability, enter or choose the name of an SLA (service level
        agreement) Monitor object that defines the monitoring policy, in the Route Tracking field.
        See SLA Monitor Objects.
Step 12  Click Ok.