Transparent or Routed Firewall Mode for Firepower Threat Defense

This chapter describes how to set the firewall mode to routed or transparent, as well as how the firewall works in each firewall mode.

Note

The firewall mode only affects regular firewall interfaces, and not IPS-only interfaces such as inline sets or passive interfaces. IPS-only interfaces can be used in both firewall modes. See Inline Sets and Passive Interfaces for Firepower Threat Defense for more information about IPS-only interfaces. Inline sets might be familiar to you as "transparent inline sets," but the inline interface type is unrelated to the transparent firewall mode described in this chapter or the firewall-type interfaces.

- About the Firewall Mode, on page 1
- Default Settings, on page 9
- Guidelines for Firewall Mode, on page 9
- Set the Firewall Mode, on page 10

About the Firewall Mode

The Firepower Threat Defense device supports two firewall modes for regular firewall interfaces: Routed Firewall mode and Transparent Firewall mode.

About Routed Firewall Mode

In routed mode, the Firepower Threat Defense device is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet.

About Transparent Firewall Mode

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or “stealth firewall,” and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place.
Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the Firepower Threat Defense device uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other.

Using the Transparent Firewall in Your Network

The Firepower Threat Defense device connects the same network between its interfaces. Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network.

The following figure shows a typical transparent firewall network where the outside devices are on the same subnet as the inside devices. The inside router and hosts appear to be directly connected to the outside router.

**Figure 1: Transparent Firewall Network**

---

Diagnostic Interface

In addition to each Bridge Virtual Interface (BVI) IP address, you can add a separate Diagnostic slot/port interface that is not part of any bridge group, and that allows only management traffic to the Firepower Threat Defense device.

Passing Traffic For Routed-Mode Features

For features that are not directly supported on the transparent firewall, you can allow traffic to pass through so that upstream and downstream routers can support the functionality. For example, by using an access rule, you can allow DHCP traffic (instead of the unsupported DHCP relay feature) or multicast traffic such as that created by IP/TV. You can also establish routing protocol adjacencies through a transparent firewall; you can allow OSPF, RIP, EIGRP, or BGP traffic through based on an access rule. Likewise, protocols like HSRP or VRRP can pass through the Firepower Threat Defense device.
About Bridge Groups

A bridge group is a group of interfaces that the Firepower Threat Defense device bridges instead of routes. Bridge groups are only supported in Transparent Firewall Mode. Like any other firewall interfaces, access control between interfaces is controlled, and all of the usual firewall checks are in place.

Bridge Virtual Interface (BVI)

Each bridge group includes a Bridge Virtual Interface (BVI). The Firepower Threat Defense device uses the BVI IP address as the source address for packets originating from the bridge group. The BVI IP address must be on the same subnet as the bridge group member interfaces. The BVI does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported.

Only bridge group member interfaces are named and can be used with interface-based features.

Bridge Groups in Transparent Firewall Mode

Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the Firepower Threat Defense device, and traffic must exit the Firepower Threat Defense device before it is routed by an external router back to another bridge group in the Firepower Threat Defense device. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a syslog server or AAA server configuration.

You can include multiple interfaces per bridge group. See Guidelines for Firewall Mode, on page 9 for the exact number of bridge groups and interfaces supported. If you use more than 2 interfaces per bridge group, you can control communication between multiple segments on the same network, and not just between inside and outside. For example, if you have three inside segments that you do not want to communicate with each other, you can put each segment on a separate interface, and only allow them to communicate with the outside interface. Or you can customize the access rules between interfaces to allow only as much access as desired.

The following figure shows two networks connected to the Firepower Threat Defense device, which has two bridge groups.
Bridge Groups in Routed Firewall Mode

Bridge group traffic can be routed to other bridge groups or routed interfaces. You can choose to isolate bridge group traffic by not assigning a name to the BVI interface for the bridge group. If you name the BVI, then the BVI participates in routing like any other regular interface.

One use for a bridge group in routed mode is to use extra interfaces on the Firepower Threat Defense device instead of an external switch. For example, the default configuration for some devices include an outside interface as a regular interface, and then all other interfaces assigned to the inside bridge group. Because the purpose of this bridge group is to replace an external switch, you need to configure an access policy so all bridge group interfaces can freely communicate.
**Figure 3: Routed Firewall Network with an Inside Bridge Group and an Outside Routed Interface**

**Allowing Layer 3 Traffic**

- Unicast IPv4 and IPv6 traffic requires an access rule to be allowed through the bridge group.
- ARPs are allowed through the bridge group in both directions without an access rule. ARP traffic can be controlled by ARP inspection.
- IPv6 neighbor discovery and router solicitation packets can be passed using access rules.
- Broadcast and multicast traffic can be passed using access rules.

**Allowed MAC Addresses**

The following destination MAC addresses are allowed through the bridge group if allowed by your access policy (see Allowing Layer 3 Traffic, on page 5). Any MAC address not on this list is dropped.

- TRUE broadcast destination MAC address equal to FFFF.FFFF.FFFF
- IPv4 multicast MAC addresses from 0100.5E00.0000 to 0100.5EFE.FFFF
- IPv6 multicast MAC addresses from 3333.0000.0000 to 3333.FFFF.FFFF
- BPDU multicast address equal to 0100.0CCC.CCCD

**BPDU Handling**

To prevent loops using the Spanning Tree Protocol, BPDUs are passed by default.
MAC Address vs. Route Lookups

For traffic within a bridge group, the outgoing interface of a packet is determined by performing a destination MAC address lookup instead of a route lookup.

Route lookups, however, are necessary for the following situations:

- Traffic originating on the Firepower Threat Defense device—Add a default/static route on the Firepower Threat Defense device for traffic destined for a remote network where a syslog server, for example, is located.
- Voice over IP (VoIP) and TFTP traffic, and the endpoint is at least one hop away—Add a static route on the Firepower Threat Defense device for traffic destined for the remote endpoint so that secondary connections are successful. The Firepower Threat Defense device creates a temporary "pinhole" in the access control policy to allow the secondary connection; and because the connection might use a different set of IP addresses than the primary connection, the Firepower Threat Defense device needs to perform a route lookup to install the pinhole on the correct interface.

Affected applications include:

- H.323
- RTSP
- SIP
- Skinny (SCCP)
- SQL*Net
- SunRPC
- TFTP

- Traffic at least one hop away for which the Firepower Threat Defense device performs NAT—Configure a static route on the Firepower Threat Defense device for traffic destined for the remote network. You also need a static route on the upstream router for traffic destined for the mapped addresses to be sent to the Firepower Threat Defense device.

This routing requirement is also true for embedded IP addresses for VoIP and DNS with NAT enabled, and the embedded IP addresses are at least one hop away. The Firepower Threat Defense device needs to identify the correct egress interface so it can perform the translation.
Unsupported Features for Bridge Groups in Transparent Mode

The following table lists the features are not supported in bridge groups in transparent mode.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic DNS</td>
<td>—</td>
</tr>
<tr>
<td>DHCP relay</td>
<td>The transparent firewall can act as a DHCPv4 server, but it does not support DHCP relay. DHCP relay is not required because you can allow DHCP traffic to pass through using two access rules: one that allows DCHP requests from the inside interface to the outside, and one that allows the replies from the server in the other direction.</td>
</tr>
</tbody>
</table>
You can, however, add static routes for traffic originating on the Firepower Threat Defense device for bridge group member interfaces. You can also allow dynamic routing protocols through the Firepower Threat Defense device using an access rule.

Multicast IP routing

You can allow multicast traffic through the Firepower Threat Defense device by allowing it in an access rule.

QoS

—

### Unsupported Features for Bridge Groups in Routed Mode

The following table lists the features are not supported in bridge groups in routed mode.

#### Table 2: Unsupported Features in Routed Mode

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic routing protocols</td>
<td>You can, however, add static routes for BVIs. You can also allow dynamic routing protocols through the Firepower Threat Defense device using an access rule.</td>
</tr>
<tr>
<td>Multicast IP routing</td>
<td>You can allow multicast traffic through the Firepower Threat Defense device by allowing it in an access rule.</td>
</tr>
<tr>
<td>QoS</td>
<td>Non-bridge group interfaces support QoS.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>VPN termination for through traffic</td>
<td>You cannot terminate a VPN connection on the BVI. Non-bridge group interfaces support VPN. Bridge group member interfaces support site-to-site VPN tunnels for management connections only. It does not terminate VPN connections for traffic through the Firepower Threat Defense device. You can pass VPN traffic through the bridge group using an access rule, but it does not terminate non-management connections.</td>
</tr>
</tbody>
</table>

**Default Settings**

**Bridge Group Defaults**

By default, all ARP packets are passed within the bridge group.

**Guidelines for Firewall Mode**

**Model Guidelines**

- For the Firepower Threat Defense Virtual on VMware with bridged ixgbevf interfaces, transparent firewall mode bridge groups are not supported.

**Bridge Group Guidelines (Transparent Mode)**

- You can create up to 250 bridge groups, with 4 interfaces per bridge group.
- Each directly-connected network must be on the same subnet.
- The Firepower Threat Defense device does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported.
- For IPv4, an IP address for the BVI is required for each bridge group for both management traffic and for traffic to pass through the Firepower Threat Defense device. IPv6 addresses are supported, but not required for the BVI.
- You can only configure IPv6 addresses manually.
- The BVI IP address must be on the same subnet as the connected network. You cannot set the subnet to a host subnet (255.255.255.255).
- Management interfaces are not supported as bridge group members.
- In transparent mode, you must use at least 1 bridge group; data interfaces must belong to a bridge group.
- In transparent mode, do not specify the BVI IP address as the default gateway for connected devices; devices need to specify the router on the other side of the Firepower Threat Defense device as the default gateway.
• In transparent mode, the default route, which is required to provide a return path for management traffic, is only applied to management traffic from one bridge group network. This is because the default route specifies an interface in the bridge group as well as the router IP address on the bridge group network, and you can only define one default route. If you have management traffic from more than one bridge group network, you need to specify a regular static route that identifies the network from which you expect management traffic.

• In transparent mode, PPPoE is not supported for the Diagnostic interface.

• Bidirectional Forwarding Detection (BFD) echo packets are not allowed through the FTD when using bridge group members. If there are two neighbors on either side of the FTD running BFD, then the FTD will drop BFD echo packets because they have the same source and destination IP address and appear to be part of a LAND attack.

## Set the Firewall Mode

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>FTD</td>
<td>Any</td>
<td>Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Access Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Network Admin</td>
</tr>
</tbody>
</table>

You can set the firewall mode when you perform the initial system setup at the CLI. We recommend setting the firewall mode during setup because changing the firewall mode erases your configuration to ensure you do not have incompatible settings. If you need to change the firewall mode later, you must do so from the CLI.

### Procedure

**Step 1**
Deregister the FTD device from the FMC.
You cannot change the mode until you deregister the device.

a) Choose Devices > Device Management.
b) Select the device from the list of managed devices.
c) Delete the device (click the Trash can icon), confirm, and wait for the system to remove the device.

**Step 2**
Access the FTD device CLI, preferably from the console port.
If you use SSH to the diagnostic interface, then changing the mode erases your interface configuration and you will be disconnected. You should instead connect to the management interface.

**Step 3**
Change the firewall mode:

`configure firewall [routed | transparent]`

**Example:**

```
> configure firewall transparent
This will destroy the current interface configurations, are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```
Step 4  Re-register with the FMC:

```
configure manager add {hostname | ip_address | DONTRESOLVE} reg_key [nat_id]
```

where:

- `{hostname | ip_address | DONTRESOLVE }` specifies either the fully qualified host name or IP address of the FMC. If the FMC is not directly addressable, use DONTRESOLVE.

- `reg_key` is the unique alphanumeric registration key required to register a device to the FMC.

- `nat_id` is an optional alphanumeric string used during the registration process between the FMC and the device. It is required if the hostname is set to DONTRESOLVE.