Firepower Data Interfaces

Cisco Defense Orchestrator (CDO) supports configuring routed interfaces and bridge virtual interfaces on Firepower Threat Defense (FTD) devices.

Routed Interfaces

Each Layer 3 routed interface (or subinterface) requires an IP address on a unique subnet. You would typically attach these interfaces to switches, a port on another router, or to an ISP/WAN gateway.

You can assign a static address, or you can obtain one from a DHCP server. However, if the DHCP server provides an address on the same subnet as a statically-defined interface on the device, the system will disable the DHCP interface. If an interface that uses DHCP to get an address stops passing traffic, check whether the address overlaps the subnet for another interface on the device.

You can configure both IPv6 and IPv4 addresses on a routed interface. Make sure you configure a default route for both IPv4 and IPv6. This task will need to be performed on the FTD device using Firepower Device Manager. See "Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version x.x.x", The Basics > Routing for information about configuring a default route.

Bridge Groups and Bridge Virtual Interfaces

A bridge group is a group of interfaces that the FTD device bridges instead of routes. Bridged interfaces belong to a bridge group, and all interfaces are on the same network. The bridge group is represented by a Bridge Virtual Interface (BVI) that has an IP address on the bridge network. Interfaces included in the bridge group are called "members."

You can route between routed interfaces and BVIs, if you name the BVI. In this case, the BVI acts as the gateway between member interfaces and routed interfaces. If you do not name the BVI, traffic on the bridge group member interfaces cannot leave the bridge group. Normally, you would name the interface so that you can route member interfaces to the Internet.

FTDs managed by Firepower Device Manager only support one bridge group, therefore, CDO can only manage that one bridge group and cannot create additional bridge groups on the device. CDO can only manage BVIs on FTDs installed directly on hardware, not on virtual FTD instances.

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. You can attach endpoints directly to bridge group member interfaces. You can also attach switches to add more endpoints to the same network as the BVI.
Passive Interfaces

Passive interfaces monitor traffic flowing across a network using a switch SPAN (Switched Port Analyzer) or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This function provides the system visibility within the network without being in the flow of network traffic. When configured in a passive deployment, the system cannot take certain actions such as blocking or shaping traffic. Passive interfaces receive all traffic unconditionally and no traffic received on these interfaces is retransmitted.

At this time, CDO has limited support for managing passive interfaces on an FTD:

- Passive interfaces must be configured on the FTD.
- Routed interfaces cannot be changed to passive interfaces and passives interfaces cannot be changed to routed interfaces using CDO.
- CDO does not identify passive interfaces in the interface table.

Related Topics

- IPv6 Addressing for Firepower Interfaces
- Guidelines and Limitations for Firepower Interface Configuration
- Configure a Physical Interface