Change the Management Interface IP Address on FTD Managed by FMC

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configure

- Configurations

Verify

Troubleshoot

Related Information

Introduction

This document describes how to change the management IP for the Firewall Threat Defense device managed by the Secure Firewall Management Center.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

Components Used

The information in this document is based on these software and hardware versions:

- Secure Firewall Management Center Virtual running version 7.2.6
- Cisco Secure Firewall Threat Defense Virtual running version 7.2.4

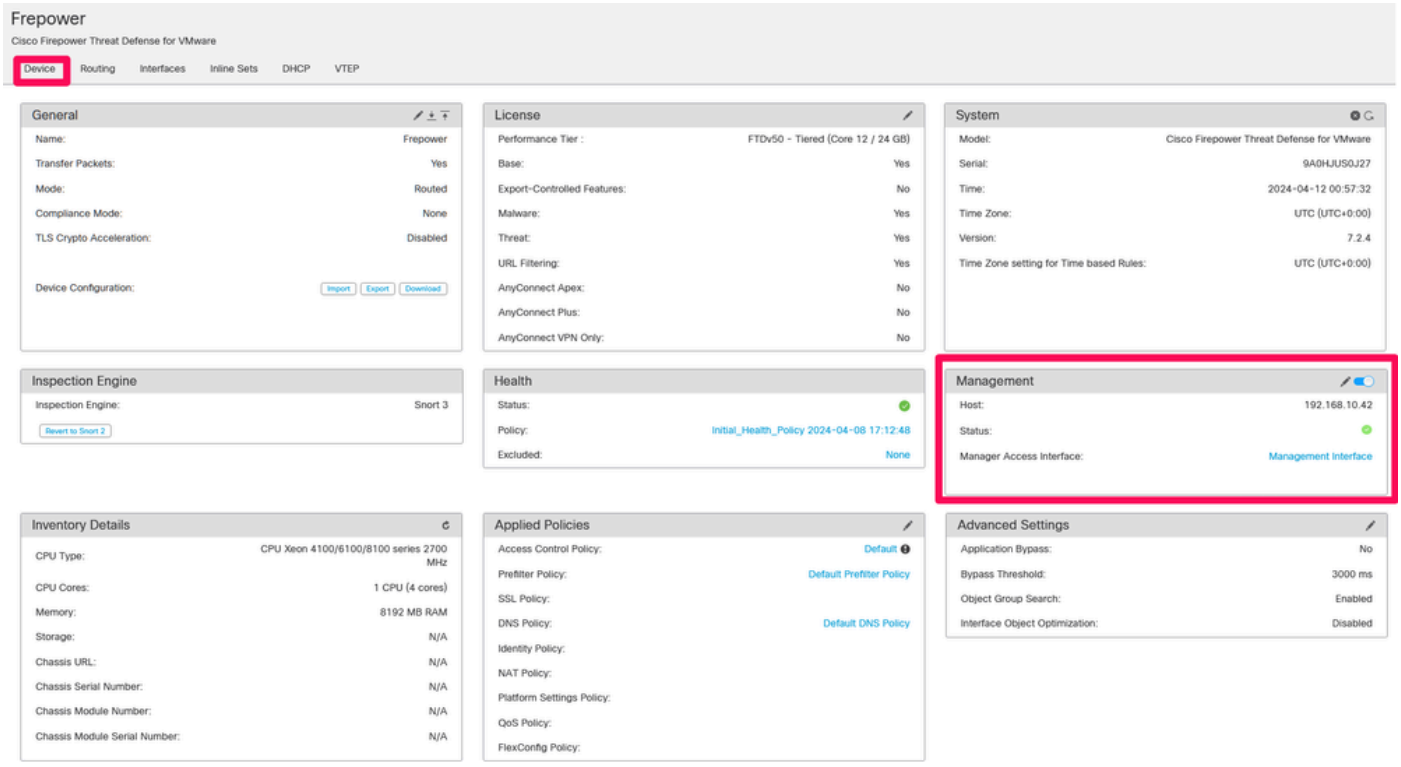
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

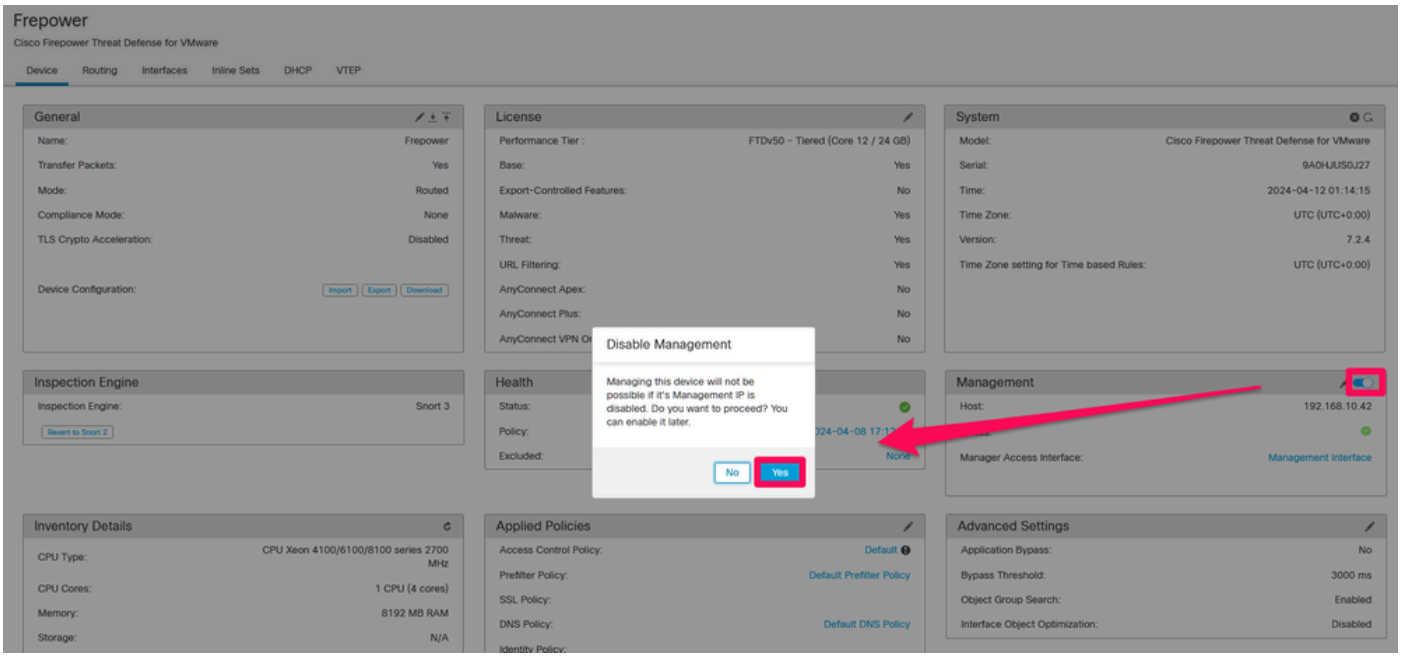
Configurations

Step 1. Navigate to the FMC GUI, and proceed to **Device > Device Management**.

Step 2. Select **Device**, and find the **Management** section.



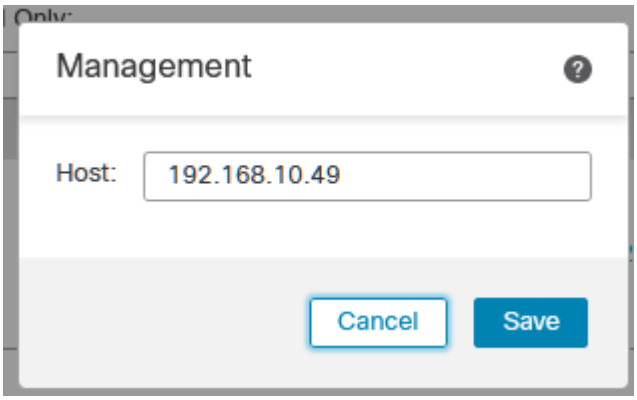
Step 3. Turn off **Management** by clicking the slider, and confirm the action by selecting **Yes**.



Note: Turning off Management halts the connection between the management center and the device, but retains the device within the management center.

Step 4. With **Management** disabled, edit the management connection by selecting **Edit**.

Step 5. In the **Management** dialog box, change the IP address in the remote **Host** address field, and then select **Save**.



Note: In case of FMC deployment in high availability, this change needs to be performed in both primary and secondary FMC appliances as this change is not replicated.

Step 6. Connect to the FTD console to modify the Management IP address.

Warning: Altering the Management IP address can result in the loss of SSH connectivity to the device if the session is established through the management IP address. Therefore, it is recommended to perform this change via Console access as suggested by Cisco.

Step 7. In Clish mode, modify the Management IP address with this command:

```
> configure network ipv4 manual 192.168.10.49 255.255.0.0 192.168.255.254
```

Note: This configuration is applied to the management interface by default.

Step 8. Return to the FMC GUI, and reactivate **Management** by toggling the Slider to the **On** position.



Step 9. Be aware that reestablishing the **Management** connection can require some time; successful reconnection is indicated as demonstrated in this image:



Verify

Use this section to confirm your configuration works properly. You can verify the Management connectivity

through the FTD CLI. This is achieved by connecting to the CLI, on Clish mode by running this command:

```
> sftunnel-status

SFTUNNEL Start Time: Fri Apr 12 01:27:55 2024
------OUTPUT OMITTED------
**********************

**RPC STATUS****192.168.10.40*************
'last_changed' => 'Fri Apr 12 01:09:19 2024',
'active' => 1,
'ipv6' => 'IPv6 is not configured for management',
'uuid_gw' => '',
'uuid' => '4a6e43f6-f5c7-11ee-97d5-a1dcfaf53393',
'name' => '192.168.10.40',
'ip' => '192.168.10.40'

Check routes:
No peers to check
```

Troubleshoot

This section provides information troubleshoot your configuration.

- To verify the management connection status at the FTD CLI, run the command **show sftunnel status brief**. Observe the output for a connection that is down, indicated by the absence of connected to details for the peer channel and missing heartbeat information.

```
> sftunnel-status-brief

PEER:192.168.10.40
Registration: Completed.
Connection to peer '192.168.10.40' Attempted at Fri Apr 19 21:14:23 2024 UTC
Last disconnect time : Fri Apr 19 21:14:23 2024 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

A healthy connection between devices is confirmed when the **sftunnel-status-brief** command at the FTD CLI produces an output that includes peer channel connected to information and heartbeat data.

```
> sftunnel-status-brief

PEER:192.168.10.40
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '192.168.10.40' via '192.168
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '192.168.10.40' via '192.168.1
Registration: Completed.
IPv4 Connection to peer '192.168.10.40' Start Time: Fri Apr 19 21:12:59 2024 UTC
```

```
Heartbeat Send Time: Fri Apr 19 21:13:00 2024 UTC
Heartbeat Received Time: Fri Apr 19 21:13:23 2024 UTC
Last disconnect time : Fri Apr 19 21:12:57 2024 UTC
Last disconnect reason : Process shutdown due to stop request from PM
```

- To check network connectivity, ping the management center from the Management interface, and enter **ping system fmc_ip** at the FTD CLI.

Related Information

- Device Management Basics
- Cisco Technical Support & Downloads