Configure FDM On-Box Management Service for Firepower 2100

Contents

Introduction

This document describes how to configure the Firepower Device Management (FDM) On-Box management service for firepower 2100 series with FTD installed.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Firepower 2100, FTD software installation.
- Cisco FTD (Firepower Threat Defense) basic configuration and troubleshooting.

Components Used

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

- Cisco Firepower 2100 series.
- Cisco FTD version 6.2.3

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.

Background Information

The main intention of this document is to guide you through the steps required to enable the FDM On-Box management for the firepower 2100 series.

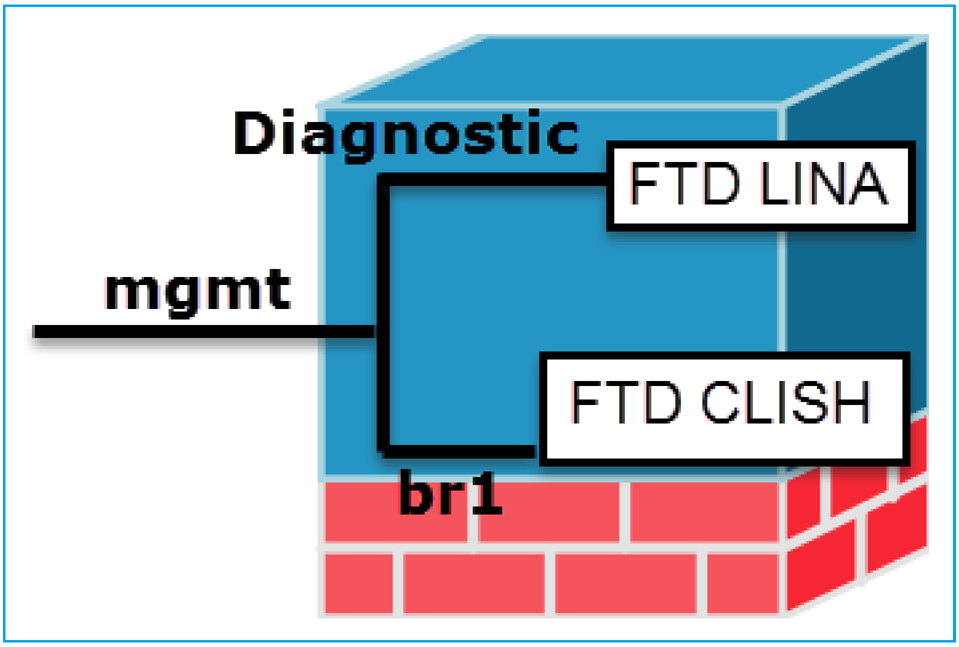
You have two options to manage the Firepower Threst Defense (FTD) installed on a firepower 2100:

- The FDM On-Box management.
- The Cisco FMC (Firepower Management Center).

Note: You cannot use both the FDM and FMC to manage an FTD installed in a firepower 2100. Once the FDM On-Box management is enabled on the firepower 2100 FTD, it is not possible to use an FMC to manage the FTD, unless you disable the local management and re-configure the management to use an FMC. On the other hand, register the FTD to an FMC disables the FDM On-Box management service on the FTD.

Caution: Right now Cisco does not have any option to migrate FDM firepower configuration to an FMC and vice-versa, take this into consideration when you choose what type of management you configure for the FTD installed in the firepower 2100.

The management interface is divided into 2 logical interfaces, br1 (management0 on FPR2100/4100/9300 appliances) and diagnostic:



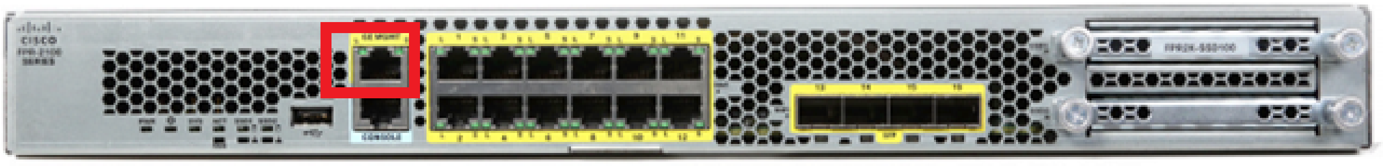
	Management - br1/management0	Management -Diagnostic
Purpose	• This interface is used in order to assign the FTD IP that is used for FTD/FMC communication. • Terminates the sftunnel between FMC/FTD. • Used as a source for rule-based syslogs. • Provides SSH and HTTPS access to the FTD box.	• Provides remote access (for example, SNM ASA engine. • Used as a source for LINA-level syslogs, A SNMP and so on messages.
Mandatory	Yes, since it is used for FTD/FMC communication (the sftunnel terminates on it).	No, and it is not recommended to conifgure it. T recommendation is to use a data interface inste (check the note below).

Note: The benefit of leaving the IP address off of the diagnostic interface is that you can place the management interface on the same network as any other data interface. If you configure the diagnostic interface, its IP address must be on the same network as the management IP address, and it counts as a regular interface that cannot be on the same network as any other data interfaces. Because the management interface requires internet access for updates, to put the management interface on the same network as an inside FTD interface means you can deploy the FTD with only a switch on the LAN and point the inside interface as the default gateway for the management interface (This just applies when the FTD is deployed in routed mode).

The FTD can be installed in a firepower 2100 appliance. The firepower chassis runs its own operating system called FXOS (Firepower eXtensible Operating System) to control basic operations of the device, while the FTD logical device is installed on a module/blade.

Note: You can use the FXOS GUI (Graphic User Interface) called FCM (Firepower Chassis Manager) or the FXOS CLI (Command Line Interface) to configure firepower chassis functions; However the GUI FCM is not available when the FTD is installed on the firepower 2100 series, just the FXOS CLI.

Firepower 21xx appliance:

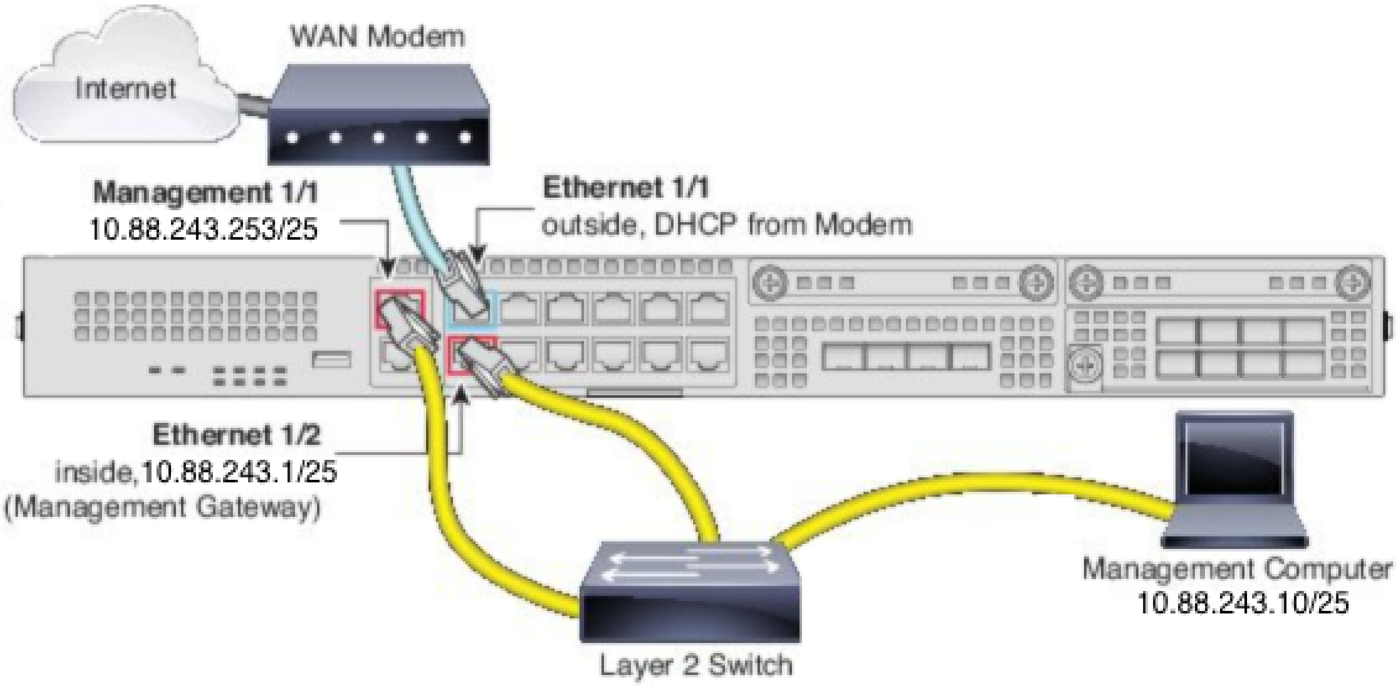


Note: On the firepower 2100 series the management interface is shared between the chassis FXOS and the FTD logical device.

Configure

Network Diagram

The default configuration assumes that certain firepower 2100 interfaces are used for the inside and outside networks. Initial configuration is be easier to complete if you connect network cables to the interfaces based on these expectations. To cable the Firepower 2100 series, see the next image.



> **Note**: The image shows a simple topology that uses a Layer 2 switch. Other topologies can be used and your deployment can vary depending on your basic logical network connectivity, ports, addressing, and configuration requirements.

Configurations

In order to enable the FDM On-Box management on the firepower 2100 series proceed as follows.

1. Console access into the FPR2100 chassis and connect to the FTD application.

```
firepower# connect ftd
>
```

2. Configure the FTD management IP address.

```
>configure network ipv4 manual 10.88.243.253 255.255.255.128 10.88.243.1
```

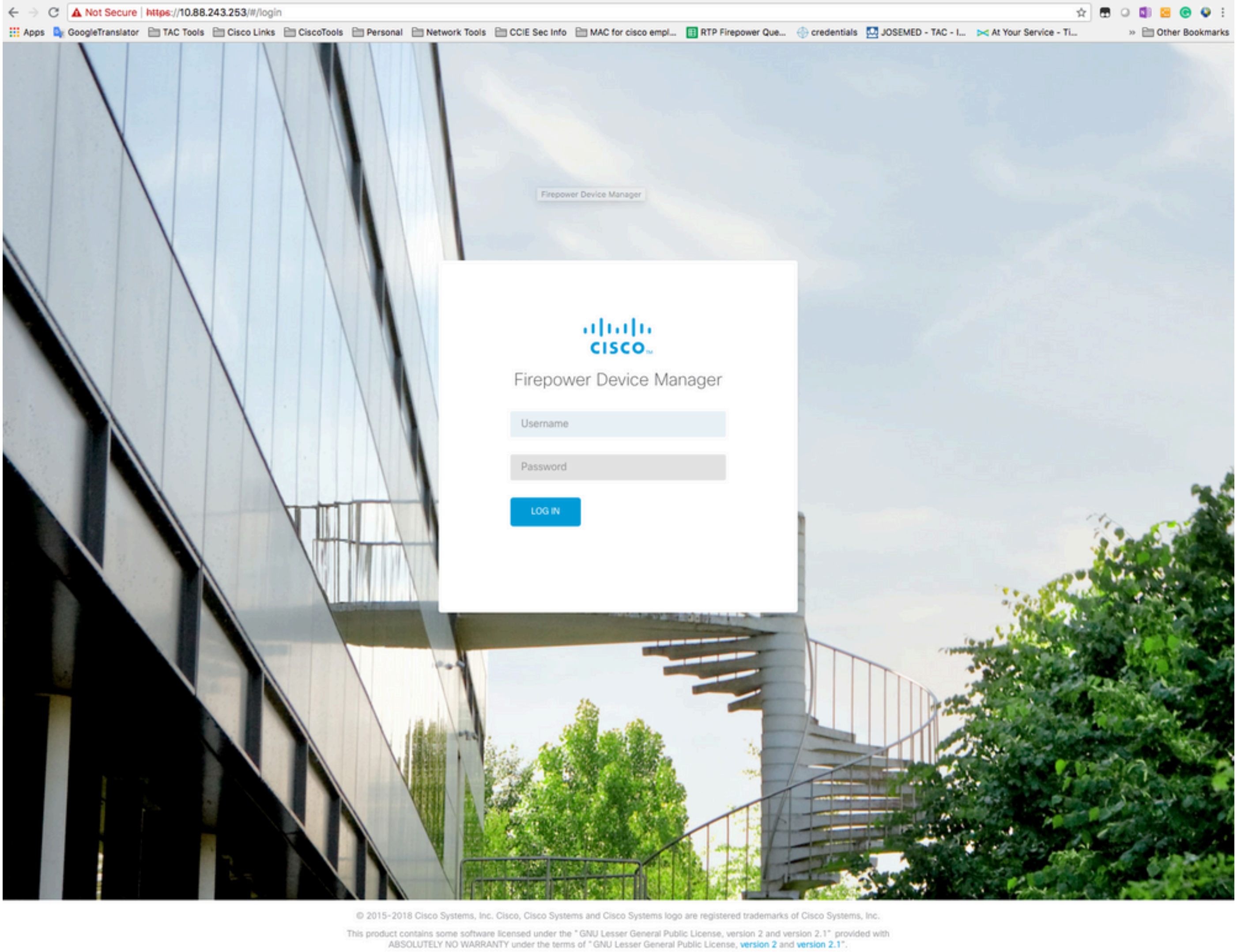
3. Configure the management type as local.

```
>configure manager local
```

4. Configure from which IP addresses/subnets the On-Box management access to the FTD can be allowed.

```
>configure https-access-list 0.0.0.0/0
```

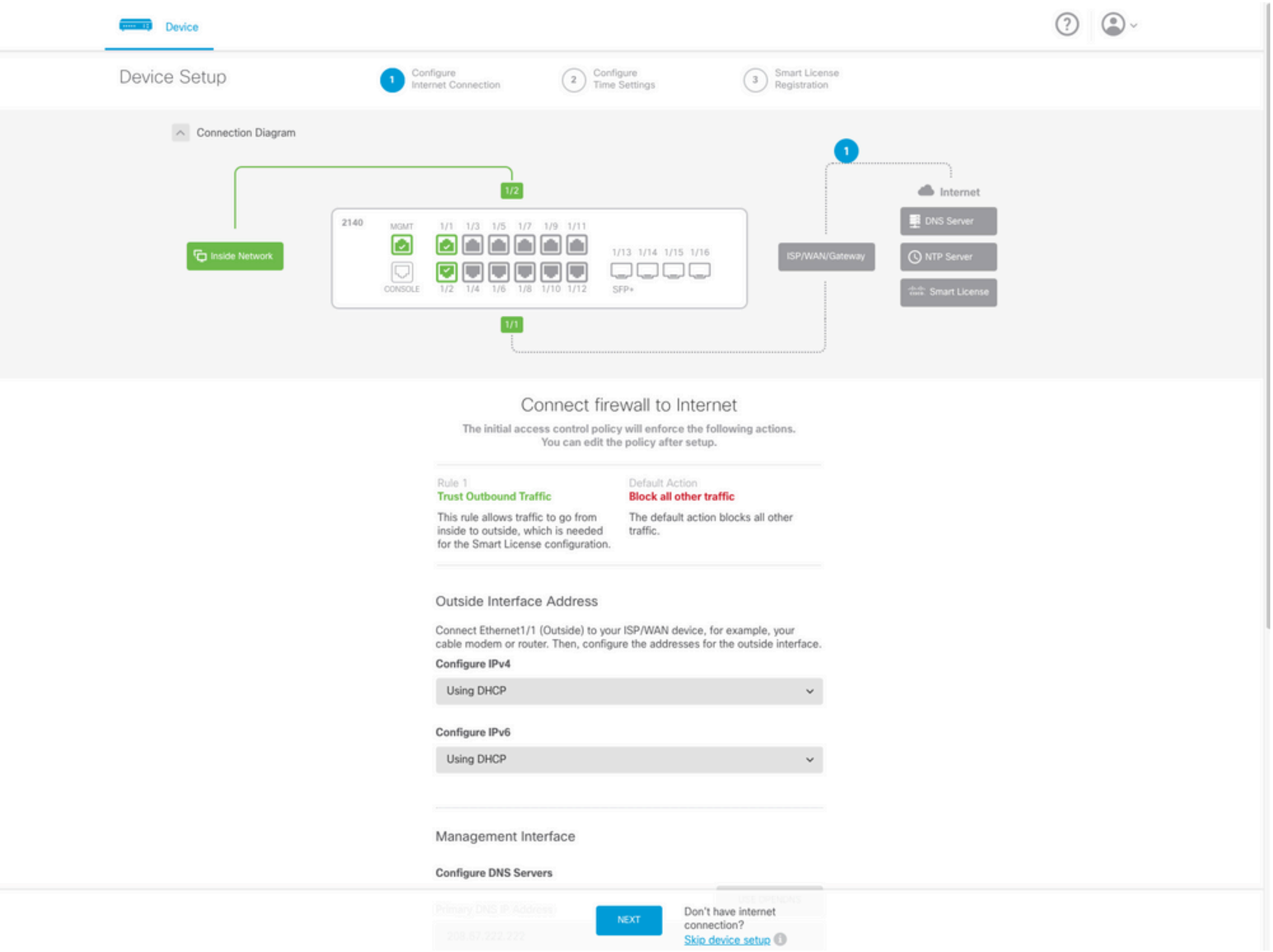
5. Open a browser and https into the IP address you configured to manage the FTD. This can open the FDM (On-Box) manager.



© 2015-2018 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc.

This product contains some software licensed under the "GNU Lesser General Public License, version 2 and version 2.1" provided with ABSOLUTELY NO WARRANTY under the terms of "GNU Lesser General Public License, version 2 and version 2.1".

6. Log in and use the default firepower credentials, username admin, and password Admin123.



Connect firewall to Internet

The initial access control policy will enforce the following actions.
You can edit the policy after setup.

Rule 1
Trust Outbound Traffic
This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration.

Default Action
Block all other traffic
The default action blocks all other traffic.

Outside Interface Address

Connect Ethernet1/1 (Outside) to your ISP/WAN device, for example, your cable modem or router. Then, configure the addresses for the outside interface.

Configure IPv4
Using DHCP

Configure IPv6
Using DHCP

Management Interface

Configure DNS Servers

NEXT

Don't have internet connection?
Skip device setup

Verify

1. Verify the network settings you configured for the FTD with the next command.

```
> show network
===============[ System Information ]===============
Hostname                  : firepower
DNS Servers               : 208.67.222.222
                            208.67.220.220
Management port           : 8305
IPv4 Default route
  Gateway                 : 10.88.243.129

==================[ management0 ]===================
State                     : Enabled
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 00:2C:C8:41:09:80
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.88.243.253
Netmask                   : 255.255.255.128
Broadcast                 : 10.88.243.255
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

```
===============[ Proxy Information ]================
State                    : Disabled
Authentication           : Disabled
```

2. Verify the management type you configured for the FTD with the next command.

```
> show managers
Managed locally.
```

Related Information

Cisco Firepower Device Manager

Cisco Firepower Threat Defense for the Firepower 2100 Series Using Firepower Management Center Quick Start Guide

Configure Firepower Threat Defense (FTD) Management Interface

Reimage the Firepower 2100 Series