

Debug: Deploy FDM VM from Azure Marketplace Using Template document in scratch

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Deploy FDM from Template on Azure Portal](#)

[Verify Configuration for VM](#)

[Check VM Deployed on Azure](#)

[Basic Configuration for FDM](#)

Introduction

This document describes deployment of Cisco Secure Firewall Threat Defense Virtual (FDM) on a virtual machine using Azure Marketplace and templates.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)
- Azure Account/Access

Components Used

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

- Cisco Secure Firewall Threat Defense Virtual versions: 7.4.1, 7.3.1, 7.2.7, 7.1.0, 7.0.6, and 6.4.0

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.

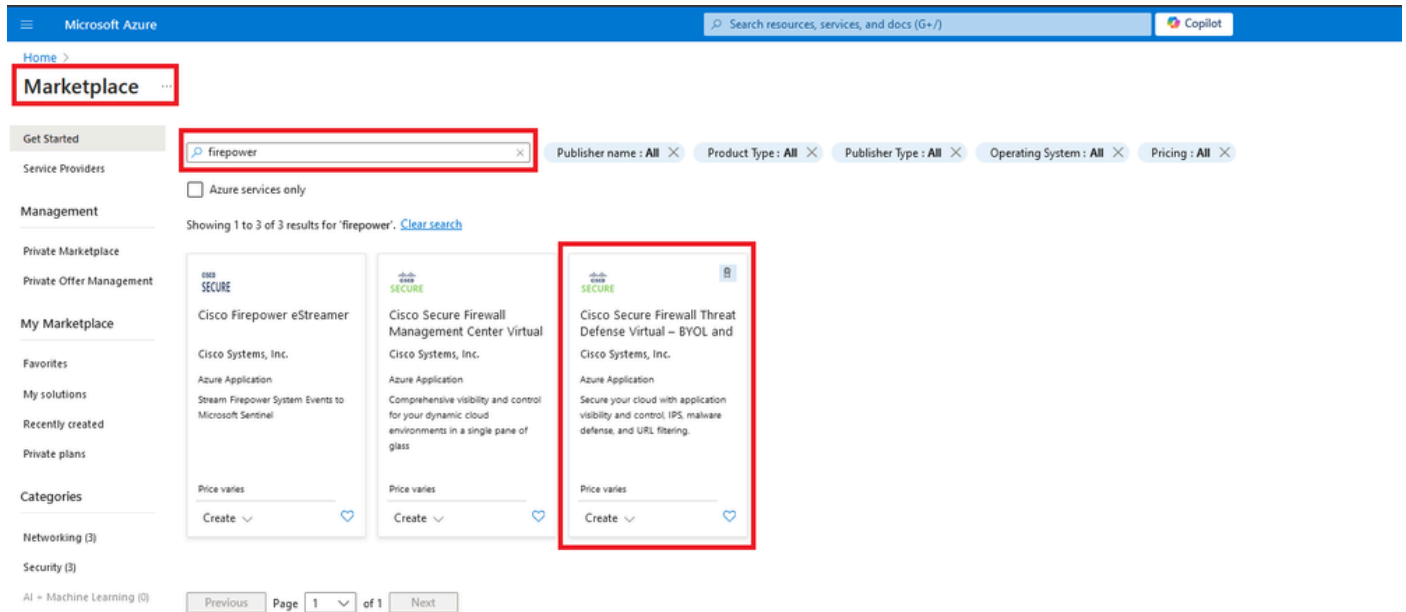
Configure

Customers have encountered issues when attempting to deploy a Firepower Device Manager (FDM) on a virtual machine from Azure, specifically when using the Azure Marketplace and templates.

Deploy FDM from Template on Azure Portal

To deploy the FDM from the Azure portal, use this procedure:

1. Navigate to the Azure portal and locate the **Marketplace** within Azure Services. Search for and select **Cisco Secure Firewall Threat Defense Virtual - BYOL and PAYG**.



Search for Firepower and Select Cisco Secure Firewall Threat Defense Virtual - BOYL

2. Click **Create** to start the configuration process for the FTD.

Home > Marketplace >

Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG

Cisco Systems, Inc.



Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG [Add to Favorites](#)

Cisco Systems, Inc. | Azure Application

★ 4.0 (2 ratings)

Microsoft preferred solution

Plan

Cisco Secure Firewall Threat Defense...

Create

- Leverage Azure Traffic Manager for highly scalable remote access VPN
- Integrate with Azure Transit VNet for scalable inter-VNet traffic

Cisco Talos® Threat Intelligence is included, protecting against known and unknown threats from one of the world's largest commercial threat intelligence teams.

[Learn more](#)

*Forrester Total Economic Impact of Cisco Secure Firewall, 2022. www.cisco.com/go/firewallTEI

More products from Cisco Systems, Inc. [See All](#)

<p>Cisco Meraki vMX Cisco Systems, Inc. Azure Application A Cisco Meraki Virtual MX to connect your Meraki network to your Azure deployments. Starts at Free Create</p>	<p>Cisco Catalyst 8000V Edge Software (PAYG) Cisco Systems, Inc. Virtual Machine Deploy and manage enterprise-class networking services and VPN technologies for the Azure cloud. Starts at \$2.53/hour Create</p>	<p>Cisco Catalyst 8000V Edge Software - Solution Cisco Systems, Inc. Azure Application Deploy and manage enterprise-class networking services and VPN technologies for the Azure cloud. Price varies Create</p>	<p>Cisco Nexus Dashboard Cisco Systems, Inc. Azure Application Simplified, centralized data center dashboard makes it easier to manage your hybrid cloud network. Price varies Create</p>
---	--	--	--

Create VM from Azure Portal

3. In the basic configuration page, create a Resource Group for the device, choose the region, and select a name for the VM.

Create Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG ...

Basics Cisco FTDv settings Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ

Instance details

Region * ⓘ

Virtual Machine name * ⓘ

Licensing ⓘ

Software Version ⓘ

A resource group is a container that holds related resources for an Azure solution.

Name *

OK Cancel

Create a new Resource Group

4. Choose the desired version for the VM deployment from the available options.

Software Version ⓘ

Availability Option * ⓘ

Username for primary account (not the FTDv admin user account) * ⓘ

Authentication type * ⓘ

7.4.1-172

7.3.1-19

7.2.7-500

7.1.0-92

7.0.6-236

6.4.0-110

Versions Available to Deploy on Azure Market

5. Set up a username for the Primary account, choose **Password** as the Authentication type, and set the Password for VM access and the Admin password.

Microsoft Azure

Home > Marketplace >

Create Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG

Basics Cisco FTDv settings Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ fw-azure

Resource group * ⓘ (New) FDM
[Create new](#)

Instance details

Region * ⓘ East US

Virtual Machine name * ⓘ fdm

Licensing ⓘ BYOL : Bring-your-own-license

Software Version ⓘ 7.4.1-172

Availability Option * ⓘ None Availability Zone

Username for primary account (not the FTDv admin user account) * ⓘ

Authentication type * ⓘ Password SSH Public Key

Password * ⓘ

Confirm password *

Admin Password * ⓘ

Confirm Admin Password * ⓘ

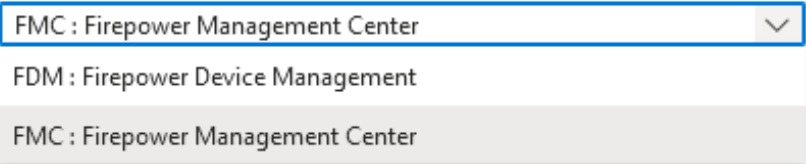
FTDv Management * ⓘ FDM : Firepower Device Management

Username and Admin Passwords.

6. For management type, select **FDM** for the purpose of this document.

FTDv Management * ⓘ

Enter FMC registration information * ⓘ



A dropdown menu with a blue border and a downward arrow on the right. The menu is open, showing three options: 'FMC : Firepower Management Center' (highlighted with a blue background), 'FDM : Firepower Device Management', and 'FMC : Firepower Management Center' (highlighted with a grey background).

Management Device.

7. In the **Cisco FTDv Settings** tab, review the VM size, Storage Account, Public IP Address, and DNS label, which are created by default after completing the basic configuration.

Ensure that the **Virtual Network**, **Management** subnet, and other **Ethernet** settings are correct.

Create Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG ...

Basics Cisco FTDv settings Review + create

Virtual machine size * ⓘ

1x Standard D3 v2
4 vcpus, 14 GB memory
[Change size](#)

Storage account * ⓘ

(new) [redacted]8b089e65
[Create New](#)

Public IP address ⓘ

(new) [redacted]-pip
[Create new](#)

DNS label ⓘ

[redacted]:352e65c ✓

.eastus.cloudapp.azure.com

Attach diagnostic interface * ⓘ

No
 Yes

Virtual network ⓘ

(New) vnet01 [redacted]FDM [redacted]
[Edit virtual network](#)

Management subnet * ⓘ

(New) subnet1
[Edit subnet](#) 172.18.0.0 - 172.18.0.255 (256 addresses)

GigabitEthernet 0/0 subnet * ⓘ

(New) subnet2
[Edit subnet](#) 172.18.1.0 - 172.18.1.255 (256 addresses)

GigabitEthernet 0/1 subnet * ⓘ

(New) subnet3
[Edit subnet](#) 172.18.2.0 - 172.18.2.255 (256 addresses)

Public inbound ports (mgmt. interface) * ⓘ

None
 Allow selected ports

i All traffic from the Internet will be blocked by default. You will be able to change inbound port rules in the VM Networking page later.

Cisco FTDv Settings.

8. Select **Allow selected Port** to enable ports SSH (22), SFTunnel (8305), and HTTPS (443) for HTTPS access to the VM and SFTunnel port for migrating the device to FMC.

Virtual network ⓘ (New) vnet01 FDM

Management subnet * ⓘ (New) subnet1
172.18.0.0 - 172.18.0.255 (256 addresses)


GigabitEthernet 0/0 subnet * ⓘ (New) subnet2
172.18.1.0 - 172.18.1.255 (256 addresses)

GigabitEthernet 0/1 subnet * ⓘ (New) subnet3
172.18.2.0 - 172.18.2.255 (256 addresses)

Public inbound ports (mgmt. interface) * ⓘ None
 Allow selected ports

Select Inbound Ports (mgmt. interface) * ⓘ 3 selected

- SSH (22)
SSH: ssh connectivity to the VM.
- SFTunnel (8305)
SFTunnel: [FMC Management]: default tcp port 8305: management center and managed device(s) communication.
- HTTPS (443)
HTTPS: [FDM Management]: FDM UI accessibility.

 Selected ports will be open for access from the Internet. See the Networking page later.

Ports to be allowed on Cisco FTDv

Verify Configuration for VM

9. Review the configuration in the **Review + Create** tab and create the VM.

Create Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG

by Cisco Systems, Inc.
[Terms of use](#) | [Privacy policy](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name	<input type="text"/>
Preferred e-mail address	<input type="text" value="@cisco.com"/>
Preferred phone number	<input type="text"/>

Basics

Subscription	<input type="text" value="fw-azure"/>
Resource group	<input type="text" value="FDM"/>
Region	East US
Virtual Machine name	<input type="text" value="fdm"/>
Licensing	BYOL : Bring-your-own-license
Software Version	7.4.1-172
Availability Option	None
Username for primary account (not the ...)	<input type="text"/>
Password	*****
Admin Password	*****
FTDv Management	FDM : Firepower Device Management

Cisco FTDv settings

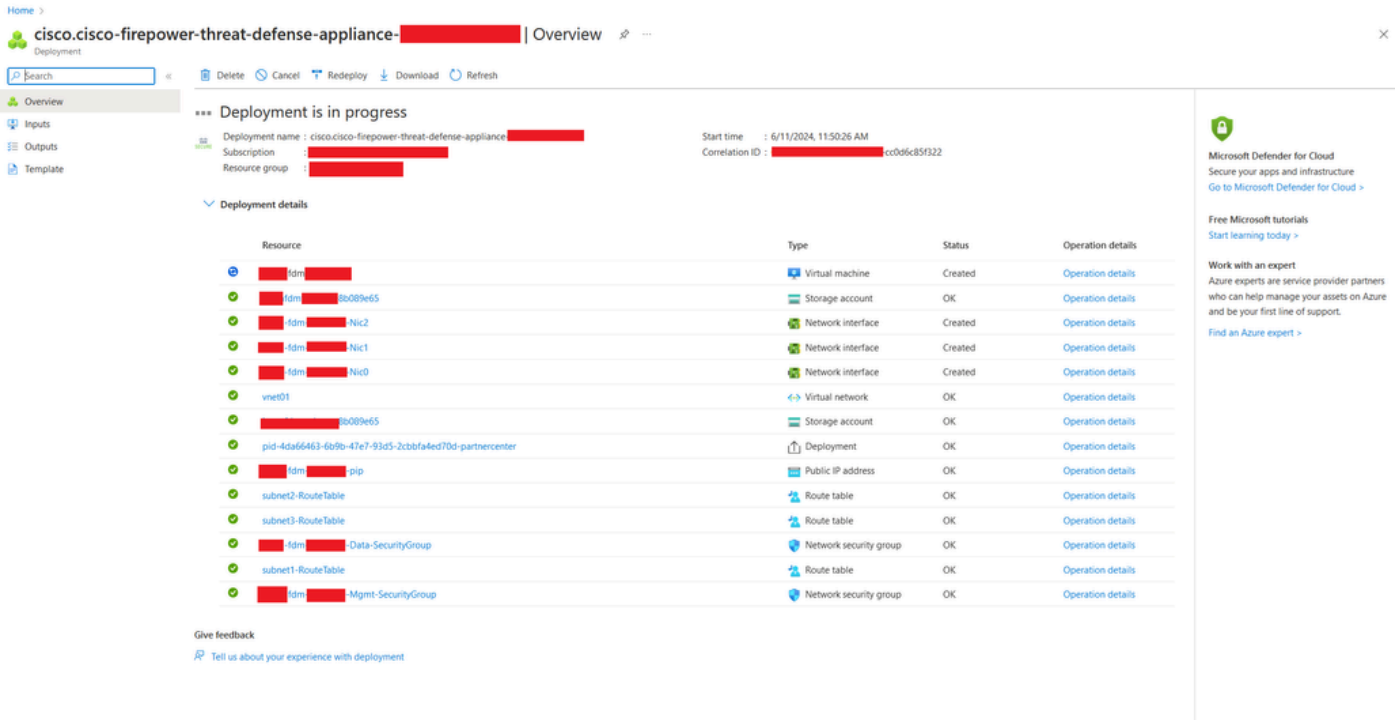
Virtual machine size	Standard_D3_v2
Storage account	<input type="text" value="8b089e65"/>
Public IP address	<input type="text" value="fdm- -pip"/>
Domain name label	<input type="text" value="-fdm- -c352e65c"/>
Attach diagnostic interface	No

Virtual network	vnet01
Management subnet	subnet1
Address prefix (Management subnet)	172.18.0.0/24
GigabitEthernet 0/0 subnet	subnet2
Address prefix (GigabitEthernet 0/0 su...)	172.18.1.0/24
GigabitEthernet 0/1 subnet	subnet3
Address prefix (GigabitEthernet 0/1 su...)	172.18.2.0/24
Public inbound ports (mgmt. interface)	Allow selected ports
Select Inbound Ports (mgmt. interface)	SSH (22), SFTunnel (8305), HTTPS (443)

Review and Create.

At this point we can submit the VM creation.

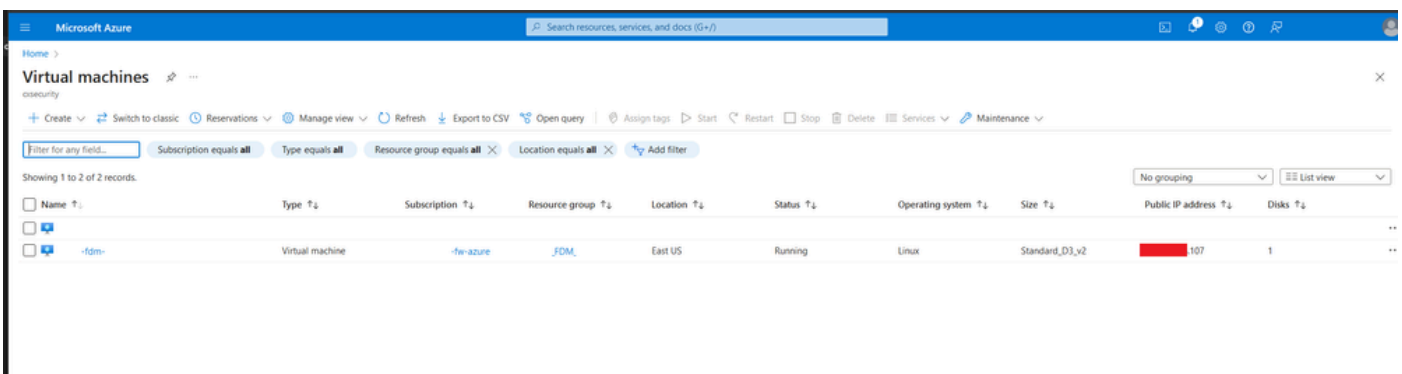
10. Monitor the deployment progress in the **Overview** tab, where a message indicates **Deployment** is in progress.



Deployment in progress.

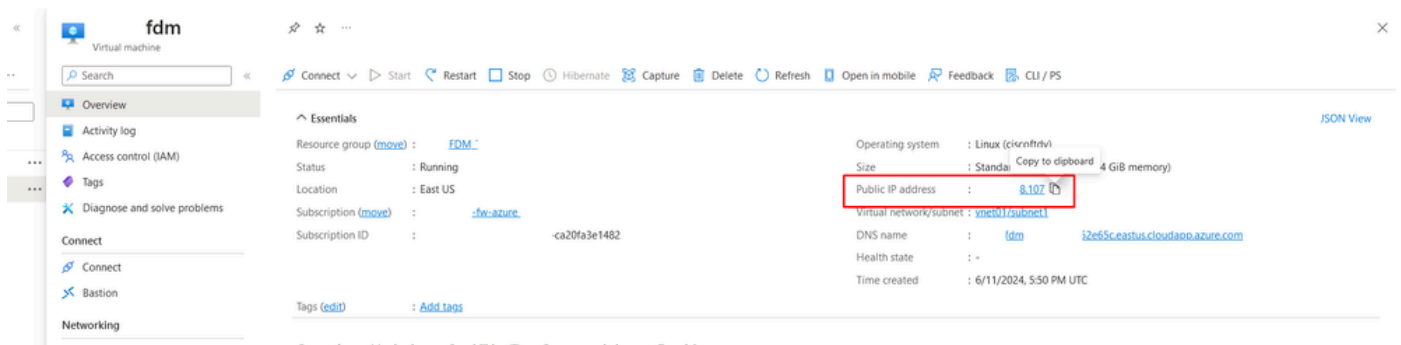
Check VM Deployed on Azure

11. When the VM is created, locate it within the **Virtual Machines** section to find its characteristics and the assigned Public IP address.



Virtual Machines Location

12. Use a browser to navigate to the assigned IP address of the device and begin the initial configuration of FDM.

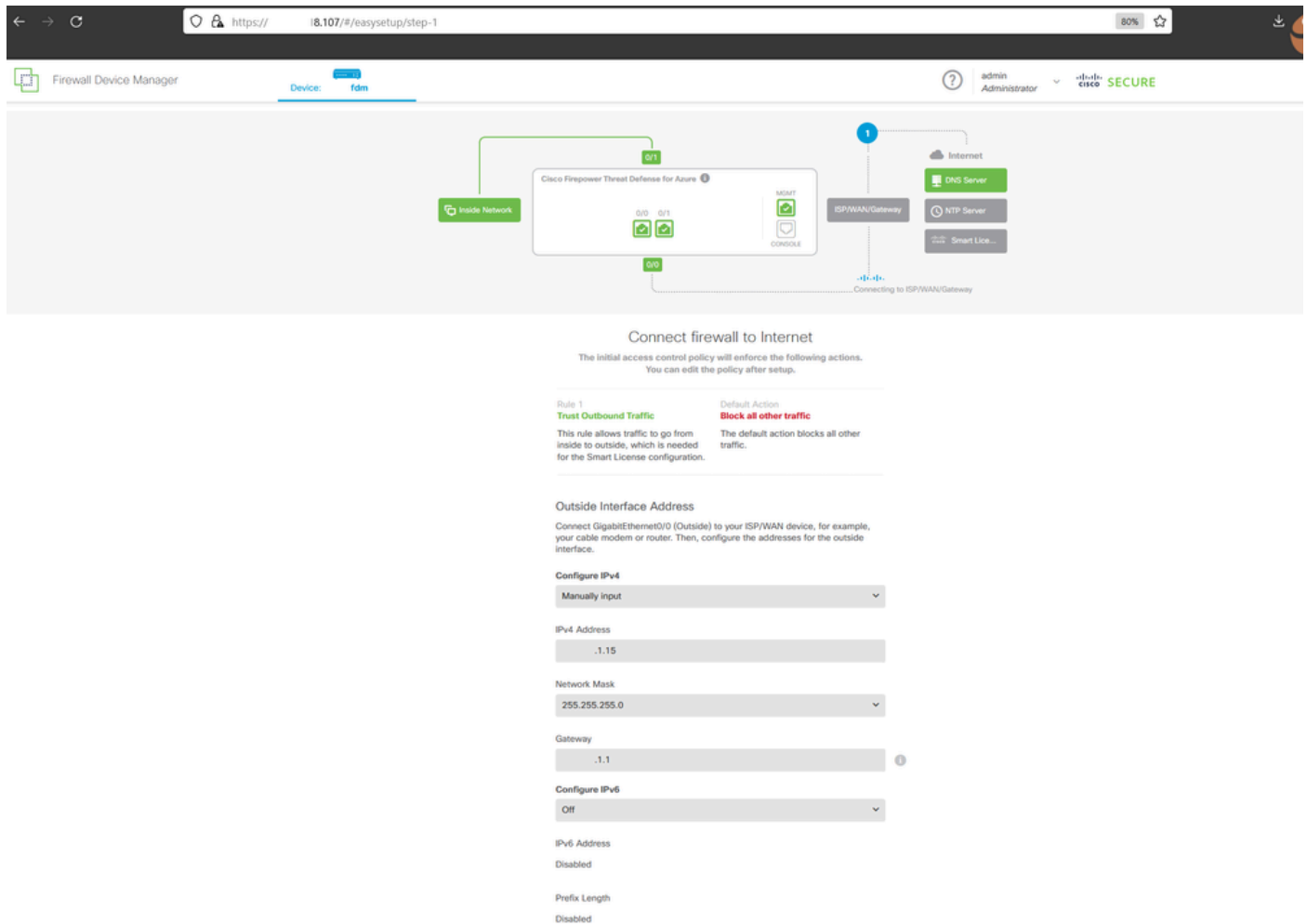


Public IP for FDM

Basic Configuration for FDM

13. Configure the basic settings by selecting an IP within the assigned range, setting up NTP, and registering the device with the license.

Here you can find the documentation for the [FDM Initial Configuration](#) .



Basic Configuration on FDM

14. After registering the device, ensure no pending deployments remain.

Pending Changes



There are no Pending Changes yet.

Nothing to deploy.

Last successful deployment was on **12 Jun 2024 07:49 AM**.

You can see what was deployed in previous jobs in the [Deployment History](#).

OK