# **Deploy FDM VM from Azure Marketplace Using Template**

### Contents

Introduction Prerequisites Requirements Components Used Configure Deploy FDM from Template on Azure Portal Verify Configuration for VM Check VM Deployed on Azure

### 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**.

$\equiv$ Microsoft Azure			٨	Search resources, ser	vices, and docs (G+/)		🔮 Copilot	
Home > Marketplace ···	l							
Get Started Service Providers		×	Publisher name : All × Pr	roduct Type : All $ imes$	Publisher Type : All $  imes $	Operating System : All $\times$	$\rm Pricing: All \ \times$	
Management	Showing 1 to 3 of 3 results for 'firepow	ver'. <u>Clear search</u>						
Private Marketplace Private Offer Management	GRD SECURE	tere SECURE	SECURE	8				
My Marketplace	Cisco Firepower eStreamer	Cisco Secure Firewall Management Center Virtual	Cisco Secure Firewall Thr Defense Virtual – BYOL a	reat and				
Favorites My solutions	Cisco Systems, Inc. Azure Application Stream Firepower System Events to	Cisco Systems, Inc. Azure Application Comprehensive visibility and control	Cisco Systems, Inc. Azure Application Secure your cloud with application	on				
Recently created Private plans	Microsoft Sentinel	for your dynamic cloud environments in a single pane of glass	visibility and control, IPS, malware defense, and URL filtering.					
Categories	Price varies Create	Price varies Create  V	Price varies Create $\checkmark$					
Security (3) Al + Machine Learning (0)	Previous Page 1 × of	1 Nevt						

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

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

≡ Micr	osoft Azure				ources, services, and docs (G+/)	🧔 Copilot		
Home > M	arketplace >							
Cisco S Cisco Systems	ecure Firewall	Threat Defense Virtu	al – BYOL and PAYG	\$2				
stada cisco SECURE	Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG Cisco Systems, Inc.   Azure Application							
	★ 4.0 (2 ratings)							
	B Microsoft preferred	solution						
• Leve • Inter Cisco Talos Learn more	Plan         Cisco Secure Firewall Threat Defense          • 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.							
*Forrester 1 More pro	fotal Economic Impact of ducts from Cisco Syste	Cisco Secure Firewall, 2022. www.cisco ems, Inc. <u>See All</u>	o.com/go/firewallTEl					
M		obolo cisco	altalo cisco	alialia cisco				
Cisco M	eraki vMX	Cisco Catalyst 8000V Edge Software (PAYG)	Cisco Catalyst 8000V Edge Software - Solution	Cisco Nexus Dashboard				
Cisco Sys	tems, Inc.	Cisco Systems, Inc.	Cisco Systems, Inc.	Cisco Systems, Inc.				
Azure App	lication	Virtual Machine	Azure Application	Azure Application				
A Cisco Me connect ye your Azure	eraki Virtual MX to our Meraki network to e deployments	Deploy and manage enterprise-class networking services and VPN technologies for the Azure cloud.	Deploy and manage enterprise-class networking services and VPN technologies for the Azure cloud.	Simplified, centralized data center dashboard makes it easier to manage your hybrid cloud network				

Create VM from Azure Portal

Starts at \$2.53/hour

Create  $\lor$ 

 $\heartsuit$ 

Price varies

Create  $\lor$ 

 $\heartsuit$ 

Starts at Free

Create  $\lor$ 

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

Price varies

Create  $\lor$ 

 $\heartsuit$ 

Ø

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

...

Project details		
Select the subscription to manage deploy manage all your resources.	ed resources and costs. Use resource groups like folders to c	organize and
Subscription * 🛈	fw-azure	$\sim$
Resource group * ①	Create new	~
Instance details Region * ①	A resource group is a container that holds related resources for an Azure solution.	~
Virtual Machine name * 🛈	Name *	_
Licensing ①	OK Cancel	~
Software Version 🕕		~

Create a new Resource Group

Basics

Cisco FTDv settings

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

Review + create

Software Version ①	7.4.1-172	$\sim$
Availability Option * ①	7.4.1-172	
	7.3.1-19	
Username for primary account (not the	7.2.7-500	
FTDv admin user account) * ①	7.1.0-92	
Authentication type * ①	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.

$\equiv$ Microsoft Azure		م
Home > Marketplace >		
Create Cisco Secure Fir	rewall Threat Defense Virtual –	BYOL and PAYG
Parine Circo CTD and inco Pari		
Basics Cisco FIDV settings Revi	ew + create	
Project details		
Select the subscription to manage deplo manage all your resources.	yed resources and costs. Use resource groups like folders t	to organize and
Subscription * ()	fw-azure	$\sim$
Resource group * ①	(New) FDM	~
	Create new	
Instance details		
Region * 🕕	East US	~
Virtual Machine name * ①	fdm	~
Licensing ①	BYOL : Bring-your-own-license	$\checkmark$
Software Version 🕕	7.4.1-172	$\sim$
Availability Option * 🕕	• None	
	Availability Zone	
Username for primary account (not the		~]
FTDv admin user account) * 🛈	. <u></u>	
Authentication type * 🛈	Password	
	SSH Public Key	
Password * ①	•••••	~
Confirm password *	•••••	~
Admin Password * ①	•••••	~
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 * 🕕	FMC : Firepower Management Center	$\sim$
Enter EMC registration information *	FDM : Firepower Device Management	
	FMC : Firepower Management Center	

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.

Home > Marketplace >

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

Basics	Cisco FTDv settings	Review + create	
Virtual m	nachine size * 🕕	<b>1x Standard D3 v2</b> 4 vcpus, 14 GB memory Change size	
Storage	account * 🕕	(new) Create New	8b089e65 V
Public IP	address ①	(new) Create new	-pip V
DNS lab	el 🛈	352	e65c 🗸
			.eastus.cloudapp.azure.com
Attach d	iagnostic interface * 🛈	<ul><li>No</li><li>Yes</li></ul>	
Virtual n	etwork ①	(New) vnet01 FDN Edit virtual network	
Manager	ment subnet * 🛈	(New) subnet1 Edit subnet	172.18.0.0 - 172.18.0.255 (256 addresses)
GigabitE	thernet 0/0 subnet * 🕕	(New) subnet2 Edit subnet	172.18.1.0 - 172.18.1.255 (256 addresses)
GigabitE	thernet 0/1 subnet * 🕕	(New) subnet3 Edit subnet	172.18.2.0 - 172.18.2.255 (256 addresses)
Public in (i)	bound ports (mgmt. interfa	ce) * <ul> <li>None</li> <li>Allow selected ports</li> </ul>	
1 AI	II traffic from the Internet will letworking page later.	be blocked by default. You will be at	le to change inbound port rules in the VM

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.



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

Preferred	e-mail	address

Preferred phone number

@cisco.com		
erisco.com		

#### Basics

Subscription	fw-azure
Resource group	FDM
Region	East US
Virtual Machine name	fdm
Licensing	BYOL : Bring-your-own-license
Software Version	7.4.1-172
Availability Option	None
Username for primary account (not the	
Password	**********
Admin Password	****
FTDv Management	FDM : Firepower Device Management

### **Cisco FTDv settings**

Virtual machine size	Standard_D3_v2
Storage account	8b089e65
Public IP address	fdm-pip
Domain name label	-fdmc352e65c
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)

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.

Home > cisco.cisco-firepower Deployment P Search «	er-threat-defense-appliance- Overview &			×
Overview     Inputs     Outputs     Outputs     Template	Deployment is in progress     Subscription     Resource group     Deployment details	Start time : 6/11/2024, 11:50:26 AM Correlation ID :		Microsoft Defender for Cloud Secure your apps and infrastructure Go to Microsoft Defender for Cloud > Free Microsoft tutorials
	Resource	Type S	tatus Operation details	Start learning today >
	Contraction of the second seco	Virtual machine C	reated Operation details	Work with an expert
	C 100 100 100 100 100 100 100 100 100 10	Storage account O	K Operation details	Azure experts are service provider partners who can help manage your assets on Azure
	I fdm	Network interface C	reated Operation details	and be your first line of support.
	I film Nic1	S Network interface C	reated Operation details	Find an Azure expert >
	International State S	Network interface C	reated Operation details	
	vnet01	↔ Virtual network 0	K Operation details	
	Ob089e65	Storage account O	K Operation details	
	pid-4da66463-6b9b-47e7-93d5-2cbbfa4ed70d-partnercenter	Deployment 0	K Operation details	
	🗢 🚺 fdm	Public IP address 0	K Operation details	
	Subnet2-RouteTable	🐴 Route table 0	K Operation details	
	Subnet3-RouteTable	📩 Route table 🛛 O	OK Operation details	
	-Idm -Data-SecurityGroup	💎 Network security group 0	OK Operation details	
	Subnet1-RouteTable	🚵 Route table 🛛 🛛 🖉	OK Operation details	
	Idm Mgmt-SecurityGroup	Network security group	OK Operation details	
	Give feedback ${\cal R}$ Teti us about your experience with deployment			

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.

Microsoft Azure			ervices, and docs (G+/)				u 🖉 🛛 🕻	d R	0
Home >									
Virtual machines 🖈 …									×
+ Create $\lor~~$ Create $\lor~~$ Switch to classic () Reservations $\lor~$	🔘 Manage view 🗸 💍 Refresh 🛓 Export to (	SV 😚 Open query 🕴 🕅	Assign tags 🕞 Start 🦿	Restart 🗌 Stop 🗊 Delet	e 💷 Services 🗸 🤌 Maint	enance 🗸			
Filter for any field Subscription equals all	Type equals all Resource group equals all X	Location equals all $\times$	⁺ <sub>♀</sub> Add filter						
Showing 1 to 2 of 2 records.							No grouping	✓ III List view	$\sim$
Name 1	Type †4 Subscription †4	Resource group †4	Location †4	Status 14	Operating system 14	Size †↓	Public IP address 14	Disks †4	
🔲 📮 -fdm-	Virtual machine -fw-azure	_FDM_	East US	Running	Linux	Standard_D3_v2	.107	1	

Virtual Machines Location

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

~	fdm Virtual machine	A &		>
	₽ Search «	🖋 Connect 🗸 ▷ Start 🤇 Restart 🔲 Stop 🕓 Hilbernate 🞉 Capture 📋 Delete 🖒 Refresh	🚺 Open in mobile 🔗 Feedback 🐻 CLI / PS	
	Overview			JSON View
	Activity log	Resource group (move) : FDM.	Operating system : Linux (ciscoffrdv)	
		Status : Running	Size : Standai Copy to dipboard 4 GiB memory)	
	Lags	Location : East US	Public IP address : 8.107	
	Diagnose and solve problems	Subscription (move) : <u>-fw-azure</u>	Virtual network/subnet : <u>vnet01/subnet1</u>	
	Connect	Subscription ID : ca20fa3e1482	DNS name : (dm 52e65c.eastus.cloudapp.azure.com	
	Ø Connect		Health state : -	
	✓ Bastion	Type (add) + Add type	Time created : 6/11/2024, 5:50 PM UTC	
	Networking			

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 <u>FDM Initial Configuration</u> .

← → C	O 🔒 https://	18.107/#/easysetup/ste	p-1				80% 公	* (
Firewall Device Manager		Device: fdm				admin Administrator	<ul> <li>"distle SECURE</li> </ul>	
			Finisde Nativort	Claco Firepower Threat Defense for Asure @		Internet		
				Connect fire The initial access control polic You can edit th	ewall to Internet sy will enforce the following actions, se 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 GigabitEthernet0/0 (Outside your cable modem or router. Then, or interface.	) to your ISP/WAN device, for example, onligure the addresses for the outside			
				Configure IPv4				
				IDul Address				
				.1.15				
				Network Mask				
				255.255.255.0	Ÿ			
				Gateway				
				Configure IPv6		0		
				Off	~			
				IPv6 Address				
				Disabled				
				Prefix Length Disabled				

Basic Confituration on FDM

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

