

FDM VM implementeren vanuit Azure Marketplace met behulp van sjabloon

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[FDM implementeren van Sjabloon op Azure Portal](#)

[Controleer de configuratie voor VM](#)

[Controleer VM geïmplementeerd in Azure](#)

[Basisconfiguratie voor FDM](#)

Inleiding

Dit document beschrijft de implementatie van Cisco Secure Firewall Threat Defence Virtual (FDM) op een virtuele machine met behulp van Azure Marketplace en sjablonen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defence (FTD)
- Azure-account/toegang

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Virtuele versies van Cisco Secure Firewall Threat Defense: 7.4.1, 7.3.1, 7.2.7, 7.1.0, 7.0.6 en 6.4.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

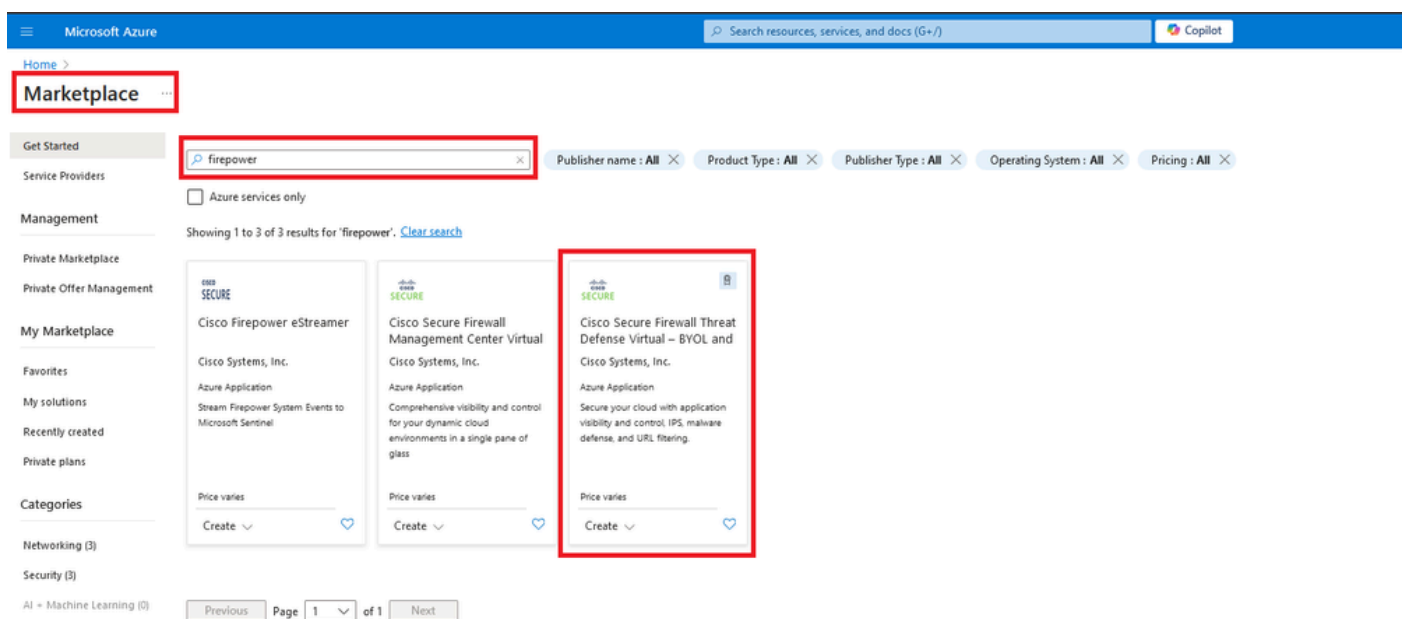
Configureren

Klanten hebben problemen ondervonden bij het inzetten van een Firepower Device Manager (FDM) op een virtuele machine van Azure, met name bij het gebruik van de Azure Marketplace en sjablonen.

FDM implementeren van Sjabloon op Azure Portal

Gebruik deze procedure om de FDM vanaf het Azure-portal te implementeren:

1. Ga naar het Azure-portal en zoek de Marketplace binnen Azure Services. Zoek naar en selecteer Cisco Secure Firewall Threat Defence Virtual - BYOL en PAYG.



Zoek naar FirePOWER en selecteer Cisco Secure Firewall Threat Defense Virtua - BYL

2. Klik op Maken om het configuratieproces voor de FTD te starten.

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>
--	--	--	---

VM maken vanuit Azure Portal

3. Maak op de pagina basisconfiguratie een resourcegroep voor het apparaat, kies de regio en selecteer een naam voor de 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

Een nieuwe resourcegroep maken

4. Kies de gewenste versie voor de VM-implementatie uit de beschikbare opties.

Software Version ⓘ

Availability Option * ⓘ

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

Authentication type * ⓘ

7.4.1-172

7.4.1-172

7.3.1-19

7.2.7-500

7.1.0-92

7.0.6-236

6.4.0-110

Versies beschikbaar voor implementatie op Azure Market

5. Stel een gebruikersnaam in voor de primaire account, kies Wachtwoord als verificatietype en stel het wachtwoord voor VM-toegang en het Admin-wachtwoord in.

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 * ⓘ [Create new](#)

Instance details

Region * ⓘ

Virtual Machine name * ⓘ

Licensing ⓘ

Software Version ⓘ

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 * ⓘ

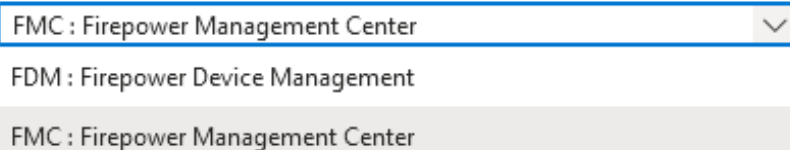
FTDv Management * ⓘ

Gebruikersnaam en Admin-wachtwoorden.

6. Selecteer voor het beheertype FDM voor de doeleinden van dit 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 in light grey), 'FDM : Firepower Device Management', and 'FMC : Firepower Management Center'.

Beheerapparaat.

7. Controleer op het tabblad Cisco FTDv Settings het VM-formaat, de opslagaccount, het openbare IP-adres en het DNS-label die standaard worden gemaakt nadat de basisconfiguratie is voltooid.

Zorg ervoor dat de instellingen van het virtuele netwerk, het beheersubstelsysteem en andere Ethernet correct zijn.

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-instellingen

8. Selecteer Toestaan dat geselecteerde poort de poorten SSH (22), SFTunnel (8305) en HTTPS (443) voor HTTPS-toegang tot de VM en SFTunnel-poort inschakelt voor de migratie van het apparaat naar 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.

Poorten die op Cisco FTDv moeten worden toegestaan

Controleer de configuratie voor VM

9. Bekijk de configuratie op het tabblad Review + Create en maak de 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)

Bekijken en maken.

Op dit moment kunnen we de VM-creatie indienen.

10. Controleer de voortgang van de implementatie op het tabblad Overzicht, waar een bericht aangeeft dat de implementatie is gestart.

Deployment overview for **cisco.cisco-firepower-threat-defense-appliance- [redacted]**. The deployment is in progress. Start time: 6/11/2024, 11:50:26 AM. Correlation ID: [redacted].

Resource	Type	Status	Operation details
[redacted] idm	Virtual machine	Created	Operation details
[redacted] idm [redacted] 3b089e65	Storage account	OK	Operation details
[redacted] idm Nic2	Network interface	Created	Operation details
[redacted] idm Nic1	Network interface	Created	Operation details
[redacted] idm Nic0	Network interface	Created	Operation details
vnet01	Virtual network	OK	Operation details
[redacted] 3b089e65	Storage account	OK	Operation details
pid-4da66463-6b9b-47e7-93d5-2cbbfa4ed70d-partnercenter	Deployment	OK	Operation details
[redacted] idm pip	Public IP address	OK	Operation details
subnet2-RouteTable	Route table	OK	Operation details
subnet3-RouteTable	Route table	OK	Operation details
[redacted] idm Data-SecurityGroup	Network security group	OK	Operation details
subnet1-RouteTable	Route table	OK	Operation details
[redacted] idm Mgmt-SecurityGroup	Network security group	OK	Operation details

Implementatie wordt uitgevoerd.

Controleer VM geïmplementeerd in Azure

11. Wanneer de VM wordt gemaakt, moet u deze in het gedeelte Virtuele machines lokaliseren om de kenmerken en het toegewezen openbare IP-adres te vinden.

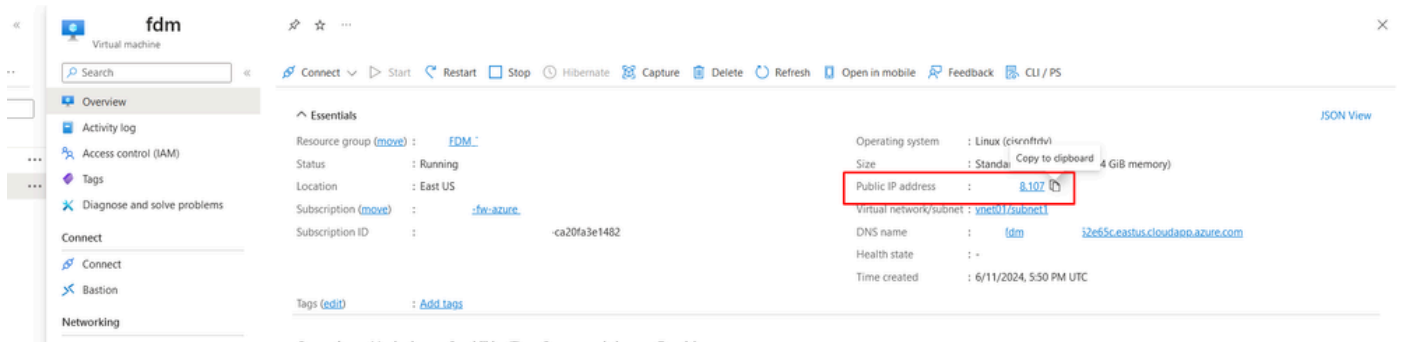
Virtual machines overview. Showing 1 to 2 of 2 records.

Name	Type	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
[redacted]	Virtual machine	-fw-azure	_FDM_	East US	Running	Linux	Standard_D3_v2	[redacted] 107	1

Locatie van virtuele machines

12. Gebruik een browser om naar het toegewezen IP-adres van het apparaat te navigeren en de

eerste configuratie van FDM te starten.



Public IP voor FDM

Basisconfiguratie voor FDM

13. Configureer de basisinstellingen door een IP te selecteren binnen het toegewezen bereik, stel NTP in en registreer het apparaat met de licentie.

Hier vindt u de documentatie voor de [FDM Initial Configuration](#).

Connect firewall to Internet

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

Rule 1	Default Action
Trust Outbound Traffic This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration.	Block all other traffic The default action blocks all other traffic.

Outside Interface Address

Connect GigabitEthernet0/0 (Outside) to your ISP/WAN device, for example, your cable modem or router. Then, configure the addresses for the outside interface.

Configure IPv4
Manually input

IPv4 Address: .1.15

Network Mask: 255.255.255.0

Gateway: .1.1

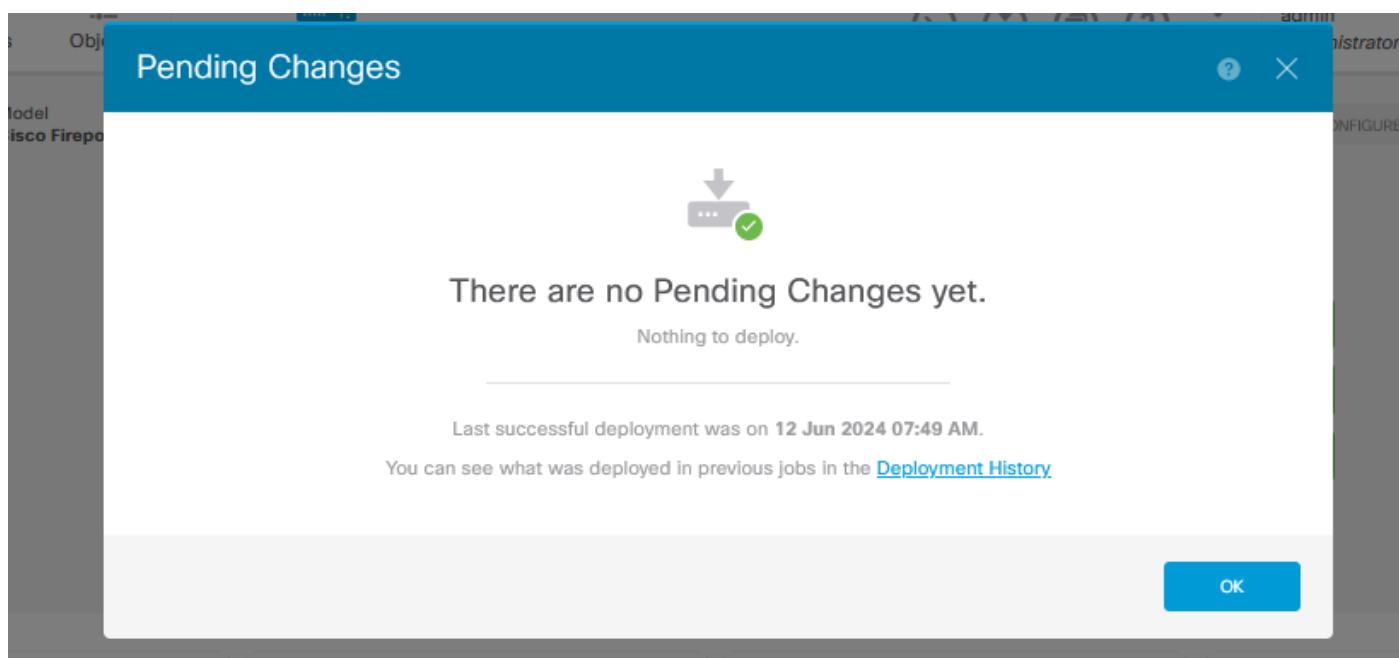
Configure IPv6
Off

IPv6 Address: Disabled

Prefix Length: Disabled

Basisconfiguratie op FDM

14. Controleer na registratie van het apparaat of er geen implementaties meer in behandeling zijn.



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.