Bereitstellen der virtuellen FDM-Maschine aus Azure Marketplace mithilfe der Vorlage

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Bereitstellung von FDM aus Vorlage im Azure-Portal Bereitstellung von FDM aus Vorlage im Azure-Portal Bereitstellung von FDM aus Vorlage im Azure-Portal Bereitstellung von FDM aus Vorlage im Azure-Portal

Einleitung

In diesem Dokument wird die Bereitstellung von Cisco Secure Firewall Threat Defense Virtual (FDM) auf einem virtuellen System mithilfe von Azure Marketplace und Vorlagen beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)
- Azure-Konto/Zugriff

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Virtuelle Versionen von Cisco Secure Firewall Threat Defense: 7.4.1, 7.3.1, 7.2.7, 7.1.0, 7.0.6 und 6.4.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Bei der Bereitstellung eines FirePOWER-Gerätemanagers (FDM) auf einem virtuellen System von Azure sind Probleme aufgetreten, insbesondere bei der Verwendung von Azure Marketplace und Vorlagen.

Bereitstellung von FDM aus Vorlage im Azure-Portal

Gehen Sie folgendermaßen vor, um den FDM über das Azure-Portal bereitzustellen:

1. Navigieren Sie zum Azure-Portal, und suchen Sie den Marketplace in Azure Services. Suchen Sie nach Cisco Secure Firewall Threat Defense Virtual - BYOL and PAYG, und wählen Sie diese Option aus.



Suchen Sie nach Firepower und wählen Sie Cisco Secure Firewall Threat Defense Virtual - BOYL

2. Klicken Sie auf Erstellen, um den Konfigurationsprozess für FTD zu starten.

= N	licrosoft Azure			⊘ Search reso	ources, services, and docs (G+/)	🕗 Copilot				
Home >	Marketplace >									
Cisco Syst	Secure Firewal	I Threat Defense Virtu	al – BYOL and PAYG	\$						
elisite cisco SECUR	cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG									
	Microsoft preferred solution									
	Plan Cisco Secure Firewall Threat Defense Create • Leverage Azure Traffic Manager for highly scalable remote access VPN									
Cisco T	alos® Threat Intelligence is	ncluded, protecting against known and	unknown threats from one of the wo	orld's largest commercial threat intelli	igence teams.					
Learn n	nore									
*Forres More	ter Total Economic Impact o products from Cisco Sys	f Cisco Secure Firewall, 2022. www.cisco tems, Inc. <u>See All</u>	o.com/go/firewallTEI							
M		Free trial	ababa cisco	ahaha cisco						
Cisco) Meraki vMX	Cisco Catalyst 8000V Edge Software (PAYG)	Cisco Catalyst 8000V Edge Software - Solution	Cisco Nexus Dashboard						
Cisco	Systems, Inc.	Cisco Systems, Inc.	Cisco Systems, Inc.	Cisco Systems, Inc.						
Azure	Application	Virtual Machine	Azure Application	Azure Application						
A Cisc conne your A	o Meraki Virtual MX to ct your Meraki network to izure 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						

VM aus Azure-Portal erstellen

C

Starts at \$2.53/ho

Create \lor

Price varies

Create \lor

 \heartsuit

Starts at Free

Create \lor

3. Erstellen Sie auf der Seite für die Basiskonfiguration eine Ressourcengruppe für das Gerät, wählen Sie die Region aus, und wählen Sie einen Namen für die VM aus.

Price varies

Create \lor

 \heartsuit

Q

Create Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG

...

Project details		
Select the subscription to manage deploy manage all your resources.	yed resources and costs. Use resource groups like folders to o	rganize and
Subscription * 🕕	fw-azure	~
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		~
Software Version ①		~

Review + create

Neue Ressourcengruppe erstellen

Basics

Cisco FTDv settings

4. Wählen Sie aus den verfügbaren Optionen die gewünschte Version für die VM-Bereitstellung aus.

Software Version 🕕	7.4.1-172	\sim
Availability Option * ①	7.4.1-172	
	7.3.1-19	
Hearnama 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	

Verfügbare Versionen für die Bereitstellung auf Azure Market

5. Richten Sie einen Benutzernamen für das primäre Konto ein, wählen Sie Kennwort als Authentifizierungstyp aus, und legen Sie das Kennwort für den VM-Zugriff und das Admin-Kennwort fest.

\equiv Microsoft Azure	۶.
Home > Marketplace >	
Create Cisco Secure Fire	ewall Threat Defense Virtual – BYOL and PAYO
Basics Cisco FIDV settings Review	w + create
Project details	
Select the subscription to manage deploy manage all your resources.	ed resources and costs. Use resource groups like folders to organize and
Subscription * ①	fw-azure V
Resource group * ①	(New) FDM V
	Create new
Instance details	
Region * ①	East US 🗸
Virtual Machine name * ①	fdm 🗸
Lieuwing ()	BVOL - Bring your own ligance
	BYOL: Bring-your-own-license
Software Version ①	7.4.1-172 ~
Availability Option * ①	None
	O Availability Zone
Username for primary account (not the FTDv admin user account) * ①	
Authentication type * ①	Password
	SSH Public Key
Password * 🕕	······
Confirm password *	······
Admin Password * 🛈	······
Confirm Admin Password * 🕕	······
FTDv Management * ①	FDM : Firepower Device Management

Benutzername und Administratorkennwörter.

6. Wählen Sie für den Verwaltungstyp FDM für dieses Dokument aus.

FTDv Management * 🕕	FMC : Firepower Management Center	\sim
Enter FMC registration information * 🕕	FDM : Firepower Device Management	
	FMC : Firepower Management Center	

Verwaltungsgerät.

7. Überprüfen Sie auf der Registerkarte Cisco FTDv Settings (Cisco FTDv-Einstellungen) die Größe des virtuellen Systems, das Speicherkonto, die öffentliche IP-Adresse und das DNS-Label, die standardmäßig nach Abschluss der Basiskonfiguration erstellt werden.

Stellen Sie sicher, dass die Einstellungen für Virtual Network, Management-Subnetz und andere Ethernet-Komponenten richtig sind.

Home > Marketplace >

Create Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG

...

Basics	Cisco FTDv settings	Review + create	
Virtual m	nachine size * 🕕	1x Standard D3 v2 4 vcpus, 14 GB memory Change size	/
Storage	account * 🛈	(new) Create New	8b089e65 ~
Public IP	address (i)	(new) Create new	-pip V
DNS lab	el 🛈	c3	52e65c 🗸
Attach d	iagnostic interface * 🛈	NoYes	.eastus.cloudapp.azure.com
Virtual n	etwork ①	(New) vnet01	M.
Manage	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	V 172.18.1.0 - 172.18.1.255 (256 addresses)
GigabitE	thernet 0/1 subnet * 🕕	(New) subnet3 Edit subnet	V 172.18.2.0 - 172.18.2.255 (256 addresses)
Public in (i)	bound ports (mgmt. interf	ace) * None Allow selected port 	S
1 A	II traffic from the Internet wi	l be blocked by default. You will be	able to change inbound port rules in the VM

Cisco FTDv-Einstellungen.

8. Wählen Sie Ausgewählten Port zulassen, um die Ports SSH (22), SFTunnel (8305) und HTTPS (443) für den HTTPS-Zugriff auf den VM- und SFTunnel-Port für die Migration des Geräts zu FMC zu aktivieren.



Zulässige Ports für Cisco FTDv

Konfiguration für VM überprüfen

9. Überprüfen Sie die Konfiguration auf der Registerkarte Prüfen + Erstellen, und erstellen Sie die 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)

Prüfen und erstellen.

An dieser Stelle können wir die Erstellung der VM einreichen.

10. Überwachen Sie den Bereitstellungsstatus auf der Registerkarte Overview (Übersicht), auf der eine Meldung angezeigt wird, dass die Bereitstellung ausgeführt wird.

Home >	· · · · ·				
cisco.cisco-firepowe Deployment	r-threat-defense-appliance-				×
	🔋 Delete 🚫 Cancel 👎 Redeploy 🛓 Download 💍 Refresh				
Overview Inputs Outputs Outputs Template	Deployment is in progress Deployment name : cisco-frepower-threat-defense-appliance Subscription Resource group Deployment details	Start time : 6/11/2024, 11:50:26 AM Constation ID :	322		Microsoft Defender for Cloud Secure your apps and infrastructure Go to Microsoft Defender for Cloud > Erea Microsoft Indelbit
	Resource	Type	Status	Operation details	Start learning today >
	e Idm	Virtual machine	Created	Operation details	Work with an expert
	Idm 60089e65	Storage account	ОК	Operation details	who can help manage your assets on Azure
	o idm Nic2	Network interface	Created	Operation details	and be your first line of support.
	-fidm -Nic1	Network interface	Created	Operation details	ring an Acute expert 2
	Sico Nico	Network interface	Created	Operation details	
	vnet01	Virtual network	ок	Operation details	
	© 1009e65	Storage account	ок	Operation details	
	pid-4da66463-6b9b-47e7-93d5-2cbbfa4ed70d-partnercenter	Deployment	OK	Operation details	
	C Internet of the second secon	Public IP address	ОК	Operation details	
	Subnet2-RouteTable	🐴 Route table	ОК	Operation details	
	Subnet3-RouteTable	😤 Route table	ок	Operation details	
	Idm Data-SecurityGroup	😵 Network security group	ок	Operation details	
	Subnet1-RouteTable	🔁 Route table	ок	Operation details	
	Idm	Network security group	ОК	Operation details	
	Give feedback $$\mathcal{R}$$ Tell us about your experience with deployment				

Bereitstellung wird ausgeführt.

VM auf Azure prüfen

11. Wenn die VM erstellt wird, suchen Sie sie im Abschnitt Virtuelle Maschinen, um ihre Merkmale und die zugewiesene öffentliche IP-Adresse zu ermitteln.

Microsoft Azure			,P Search resources, s	ervices, and docs (G+/)				d 🖓 🛛	0 R	6
Nome > Virtual machines										×
+ Create \lor 2 Switch to classic (3) Reservations \lor	🔘 Manage view 🗸 🕻) Refresh 🞍 Export to CSV 📍	🖁 Open query 📗 🖉	Assign tags 🕞 Start 🦿	Restart 🔲 Stop 🗊 Delete	III Services 🗸 🤌 Mainte	nance 🗸			
Filter for any field	Type equals all Re	source group equals all $ imes$. L	ocation equals all $ imes$	*y Add filter						
Showing 1 to 2 of 2 records.								No grouping	✓ III List view	×
Name 1.	Type ↑↓	Subscription ↑↓	Resource group 1+	Location †4	Status ↑↓	Operating system 14	Size †4	Public IP address 14	Disks †4	
-fdm-	Virtual machine	-fw-azure	_FDM_	East US	Running	Linux	Standard_D3_v2	.107	1	

Standort virtueller Systeme

12. Navigieren Sie in einem Browser zur zugewiesenen IP-Adresse des Geräts, und beginnen Sie

mit der Erstkonfiguration von FDM.

«	Control Contro	<i>\$</i> ☆ …		×
	₽ Search «	🖋 Connect 🗸 ▷ Start 🤇 Restart 🔲 Stop 🕓 Hilbernate 🎉 Capture 📋 Delete 🖒 Refresh 🔋	Open in mobile 🔗 Feedback 🐻 CLI / PS	
-	Overview	A found to		ICON IN
	Activity log	C Essentials		JSON VIEW
		Resource group (move) : EDM	Operating system : Linux (ciscoftdv)	
	Access control (IAM)	Status : Bunning	Size : Standa, Copy to dipboard 4 GiB memory)	
	🥏 Tags	Location : East US	Public IP address : 8.107	
	X 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	
	connect		Health state : -	
	S Connect			
	× Bastion	Taos (edit) : Add taos	Time created : 6/11/2024, 5:50 PM UIC	
	Networking			

Öffentliche IP für FDM

Basiskonfiguration für FDM

13. Konfigurieren Sie die Grundeinstellungen, indem Sie eine IP innerhalb des zugewiesenen Bereichs auswählen, NTP einrichten und das Gerät mit der Lizenz registrieren.

Hier finden Sie die Dokumentation zur Erstkonfiguration des FDM .

← → C	O 🏝 https://	18.107/#/easysetup/step	o-1				80% 🟠	*
Firewall Device Manager		Device: fdm				admin Administrator	 - abate cisco SECURE 	
			For Inside Network	Claco Fingover Threat Defance for Asure (00 0'1 0 0'1 00		etrony:		
				Connect fire The initial access control polic You can edit ti	ewall to Internet cy will enforce the following actions. he 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, c interface.) to your ISP/WAN device, for example, onligure the addresses for the outside			
				Configure IPv4 Manually input				
				IDul Address				
				.1.15				
				Network Mask				
				255.255.255.0	•	•		
				Gateway				
				.1.1		0		
				Configure IPv6 Off				
				IPv6 Address Disabled				
				Prefix Length Disabled				

14. Stellen Sie nach der Registrierung des Geräts sicher, dass keine ausstehenden Bereitstellungen bestehen bleiben.

-			aum	<u>.</u>
; Obj	Pending Changes	0	×	nistrator
lodel isco Firepo				NFIGURE
	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			
		ОК		

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.