使用模板從Azure應用商店部署FDM VM

目錄

 簡介

 必要條件

 憲求

 採用元件

 設定

 從Azure入口網站上的範本部署FDM

 驗證虛擬機器配置

 檢查在Azure上部署的VM

 FDM的基本組態

簡介

本文檔介紹使用Azure Marketplace和模板在虛擬機器上部署Cisco Secure Firewall Threat Defense Virtual (FDM)。

必要條件

需求

思科建議您瞭解以下主題:

- 思科安全防火牆管理中心(FMC)
- 思科安全防火牆威脅防禦(FTD)
- Azure帳戶/訪問許可權

採用元件

本檔案中的資訊是根據以下軟體版本:

- 思科安全防火牆威脅防禦虛擬版本: 7.4.1、7.3.1、7.2.7、7.1.0、7.0.6和6.4.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

設定

客戶嘗試從Azure在虛擬機器上部署Firepower裝置管理器(FDM)時遇到問題,特別是在使用Azure Marketplace和模板時。

從Azure入口網站上的範本部署FDM

若要從Azure入口網站部署FDM,請使用此程式:

1. 導航到Azure門戶,並在Azure服務中找到市場。搜尋並選擇Cisco安全防火牆威脅防禦虛擬-BYOL和PAYG。



搜尋Firepower並選擇Cisco Secure Firewall Threat Defense Virtua - BOOL

2. 按一下「建立」以開始FTD的組態程式。

	Microsoft Azure			🔎 Search reso	purces, services, and docs (G+/)	🤣 Copilot		
Hom	Home > Marketplace >							
Cisco	co Secure Firewall	Threat Defense Virtu	al – BYOL and PAYG	s?				
ab	Cisco Secure	Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG 🗢 Add to Favorites						
SEC	URE Cisco Systems, Inc. Azu	Cisco Systems, Inc. Azure Application						
	* 4.0 (2 ratings)							
	Microsoft preferred solution							
	Plan Cisco Secure Firewall Threat Defense V							
<i>C</i> -	Leverage Azure Traffic Manage Integrate with Azure Transit VN	for highly scalable remote access VF et for scalable inter-VNet traffic	'N	1.41- 1				
Lea	m more	udeo, protecting against known and	unknown uneats norn one of the wor	ia siargest commercial threat inten	gence coms.			
*Fo	rrester Total Economic Impact of C	isco Secure Firewall, 2022. www.cisco	o.com/go/firewallTEl					
Mo	re products from Cisco Syste	ms, Inc. <u>See All</u>						
	M	tree trial	alualu cisco	altala cisco				

Μ	Free trial	cisco	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 Cisco Meraki Virtual MX to connect your Meraki network to your Azure 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
Starts at Free	Starts at \$2.53/hour	Price varies	Price varies
Create 🗸 🗢 🗢	Create 🗸 💙	Create 🗸 💙	Create 🗸 🗢 🗢

從Azure門戶建立VM

3. 在基本配置頁面中,為裝置建立資源組,選擇區域,然後為VM選擇名稱。

Create Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG

...

Project details		
Select the subscription to manage dep manage all your resources.	loyed resources and costs. Use resource groups like folders to or	ganize 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		~
Software Version 🕕	OK Cancel	~

建立新的資源群組

4. 從可用選項中選擇所需的虛擬機器部署版本。

Basics Cisco FTDv settings Review + create

Software Version 🕕	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	

可在Azure Market上部署的版本

5. 設定「主要」帳戶的使用者名稱,選擇口令作為身份驗證型別,並設定VM訪問口令和管理口令。

\equiv Microsoft Azure		م				
Home > Marketplace >						
Create Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG						
Basics Cisco FTDv settings Revie	Basics Cisco FTDv settings Review + create					
Project details	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	\sim				
Resource group * ①	(New) FDM	\sim				
	Create new					
Instance details						
Region * ①	East US	\sim				
Virtual Machine name *	fdm					
	IGH					
Licensing ()	BYOL : Bring-your-own-license	\sim				
Software Version ①	7.4.1-172	\sim				
Availability Option * 🕕	None					
	O Availability Zone					
Username for primary account (not the FTDv admin user account) * ①		~				
Authentication type * ①	Password					
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	SSH Public Key					
Password * ①	•••••	~				
Confirm password *	•••••					
Admin Password * 🕕	•••••	~				
Confirm Admin Password *	••••••	\checkmark				
FTDv Management * 🕕	FDM : Firepower Device Management	\sim				

使用者名稱和管理員密碼。

6. 對於管理型別,選擇FDM作為本文檔的目的。

FTDv Management * 🕕

FMC : Firepower Management Center \sim FDM : Firepower Device Management Enter FMC registration information * ① FMC : Firepower Management Center

管理裝置。

7. 在Cisco FTDv Settings頁籤中,檢視VM大小、儲存帳戶、公共IP地址和DNS標籤(完成基本配 置後,預設情況下會建立)。

確保虛擬網路、管理子網和其他乙太網設定正確。

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 memor Change size	y
Storage	account * 🕕	(new) Create New	8b089e65 V
Public IP	address ①	(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 Filler	DM.
Manager	ment subnet * 🕕	(New) subnet1 Edit subnet	V 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	bound ports (mgmt. interfa	ace) * None Allow selected port 	s
1 A	II traffic from the Internet will etworking page later.	be blocked by default. You will be	able to change inbound port rules in the VM

Cisco FTDv Settings。

8. 選擇Allow selected Port以啟用埠SSH (22)、SFTunnel (8305)和HTTPS (443),從而透過 HTTPS訪問虛擬機器並將SFTunnel埠遷移到FMC。

Edit virtual network	
(New) subnet1	~
Edit subnet	172.18.0.0 - 172.18.0.255 (256 addresses)
(New) subnet2	~
Edit subnet	172.18.1.0 - 172.18.1.255 (256 addresses)
(New) subnet3	\sim
Edit subnet	172.18.2.0 - 172.18.2.255 (256 addresses)
 None Allow selected ports 	
3 selected	\sim
SSH (22) SSH: ssh connectivity	r to the VM.
SFTunnel (8305) SFTunnel: [FMC Man and managed device HTTPS (443) HTTPS: [FDM Manag	agement]: default tcp port 8305: management center (s) communication. ement]: FDM UI accessibility.
	idit subnet (New) subnet2 idit subnet (New) subnet3 idit subnet O None Allow selected ports 3 selected SSH (22) SSH: ssh connectivity SFTunnel (8305) SFTunnel: [FMC Man and managed device HTTPS (443) HTTPS: [FDM Managed

Cisco FTDv上允許的連線埠

驗證虛擬機器配置

9. 在Review + Create頁籤中檢視配置並建立虛擬機器。

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)

此時,我們可以提交虛擬機器建立。

10. 在概覽頁籤中監視部署進度,該頁籤上將顯示一條消息,指示部署正在進行。

Home >					
	er-threat-defense-appliance-				×
₽ Search «	🔋 Delete 🚫 Cancel 🚏 Redeploy 🛓 Download 🖒 Refresh				
👃 Overview	Deployment is in progress				
Inputs	Deployment is in progress				0
S≣ Outputs	Deployment name : cisco.cisco-tirepower-threat-defense-appliance	Start time : 6/11/2024, 11:50:26 AM Correlation ID : cc0di6c85f	322		Microsoft Defender for Cloud
E Template	Resource group :				Secure your apps and infrastructure
					Go to Microsoft Defender for Cloud >
	V Deployment details				Free Microsoft tutorials
	Resource	Туре	Status	Operation details	Start learning today >
	C Internet Contraction	Virtual machine	Created	Operation details	Work with an expert Azure experts are service provider partners
	C Internet 86089e65	Storage account	OK	Operation details	who can help manage your assets on Azure
	Idministration -Nic2	Network interface	Created	Operation details	and be your first line of support.
	S Internet Nict	Network interface	Created	Operation details	The off state support of
	C Idm Nico	Network interface	Created	Operation details	
	vnet01	Virtual network	ок	Operation details	
	C Bible Bibl	Storage account	ок	Operation details	
	pid-4da66463-6b9b-47e7-93d5-2cbbfa4ed70d-partnercenter	Deployment	OK	Operation details	
	C fdm-spip	Public IP address	ок	Operation details	
	Subnet2-RouteTable	📩 Route table	ок	Operation details	
	Subnet3-RouteTable	📩 Route table	ок	Operation details	
	Contraction - Data-SecurityGroup	Network security group	ок	Operation details	
	Subnet1-RouteTable	🐴 Route table	ок	Operation details	
	Idm-Mgmt-SecurityGroup	Network security group	ок	Operation details	
	Give feedback				
	R ² Tell us about your experience with deployment.				

部署進行中.

檢查在Azure上部署的VM

11. 建立虛擬機器後,在虛擬機器部分找到該虛擬機器,以便查詢其特性和分配的公用IP地址。

					_		_ 0 -	- -	0
Microsoft Azure		,P Search resources, se	ervices, and docs (G+/)				51 🖓 🐵	0 R	8
Home >									
Virtual machines 🖈 …									×
+ Create $\lor~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~$	🕽 Manage view 🗸 🜔 Refresh 🛓 Export to CSV	😵 Open query 👘 🖉	Assign tags 🕞 Start 🤇	Restart 🗌 Stop 🗊 Del	ete 🗉 Services 🗸 🤌 Mainte	nance 🗸			
Filter for any field	rpe equals all Resource group equals all X	Location equals all \times	⁺ _V Add filter						
Showing 1 to 2 of 2 records.							No grouping	✓ III List view	~
□ Name ↑	rpe ↑↓ Subscription ↑↓	Resource group 12	Location †4	Status 14	Operating system ↑↓	Size ↑↓	Public IP address 1+	Disks †4	
🗌 📮 -fdm- Vi	itual machine -fw-azure	(FDM)	East US	Running	Linux	Standard_D3_v2	.107	1	

虛擬機器器位置

12. 使用瀏覽器瀏覽至裝置指派的IP位址,並開始初始設定FDM。

~	fdm Virtual machine	\$ * ···	×
	₽ Search «	🖋 Connect 🗸 ▷ Start 🤇 Restart 🔲 Stop 🕓 Hilbernate 🎉 Capture 👔 Delete 🖒 Refresh 🏮 Open in mobile 🔗 Feedback 👼 CLI / PS	
	Overview		JSON View
	Activity log	Parenter a rente (mens) 1 ENL ⁺	
	Access control (IAM)	Status : Running Size : Standa Copy to dipboard 4 GiB memory)	
	🥏 Tags	Location : East US Public IP address : 8.102 05	
	X Diagnose and solve problems	Subscription (move) : <u>:fw-azure</u> . Virtual network/subnet : <u>vnet01/subnet1</u>	
	Connect	Subscription ID : -ca20fa3e1482 DNS name : Idm i22e55ceastus.cloudaop.azute.com	
	Ø Connect	Health state : -	
		Time created : 6/11/2024, 5:50 PM UTC	
	Networking	Tags (edit) : Add.tags	

FDM的公用IP

FDM的基本組態

13. 透過選擇分配範圍內的IP、設定NTP並在許可證中註冊裝置來配置基本設定。

您可以在此處找到<u>FDM初始配置</u>的文檔。

← → C	O 🔒 https://	18.107/#/easysetup/ste	p-1					80%	* (
Firewall Device Manager		Device: fdm					admin Administrator	esco SECURE	
			C Inside Network	Cisco Firepower Thread Defense for Anne C Cisco Firepower Thread Defense for Anne C Cisco Firepower Thread Defense for Anne C Cisco Firepower Thread Defense for Anne C		AMAN Gases	MTP Server		
				Connect fire The initial access control polic You can edit th Rule 1 Trust Outbound Traffic This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration.	y will enforce the following active policy after setup.	ons.			
				Outside Interface Address Connect GigabitEthernet0/0 (Outside your cable modem or router. Then, o interface. Configure IPv4 Manually innut) to your ISP/WAN device, for exa onligure the addresses for the out	mple, side			
				IPv4 Address .1.15 Network Mask 255.255.255.0		v			
				Gateway .1.1 Configure IPv6 Off		×	0		
				IPv6 Address Disabled Prefix Length Disabled					
FDM的基本配置									

14. 註冊裝置後,請確保不再保留任何待處理的部署。



關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。