使用模板从Azure应用商店部署FDM VM

目录

 節介

 先决条件

 要求

 使用的组件

 配置

 从Azure门户上的模板部署FDM

 验证虚拟机的配置

 检查在Azure上部署的VM

 FDM的基本配置

简介

本文档介绍使用Azure应用商店和模板在虚拟机上部署Cisco Secure Firewall Threat Defense Virtual (FDM)。

先决条件

要求

Cisco 建议您了解以下主题:

- 思科安全防火墙管理中心(FMC)
- 思科安全防火墙威胁防御(FTD)
- Azure帐户/访问权限

使用的组件

本文档中的信息基于以下软件版本:

- 思科安全防火墙威胁防御虚拟版本: 7.4.1、7.3.1、7.2.7、7.1.0、7.0.6和6.4.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

配置

客户在尝试从Azure在虚拟机上部署Firepower设备管理器(FDM)时遇到问题,特别是在使用Azure应 用商店和模板时。

从Azure门户上的模板部署FDM

要从Azure门户部署FDM,请使用以下步骤:

1. 导航到Azure门户并在Azure服务中找到市场。搜索并选择Cisco Secure Firewall Threat Defense Virtual - BYOL and PAYG。



搜索Firepower并选择Cisco Secure Firewall Threat Defense Virtua - BOM

2. 单击创建以开始FTD的配置过程。

	Microsoft Azure				urces, services, and docs (G+/)	🔕 Copilot
Home	> Marketplace >					
Cisco S	co Secure Firewall	Threat Defense Virtu	ual – BYOL and PAYG	s?		
alta	Cisco Secure	Firewall Threat Def	ense Virtual – BYOL	and PAYG 🛇 Add to Favo	prites	
SEC	URE Cisco Systems, Inc. Azu	re Application				
	★ 4.0 (2 ratings)					
	A Microsoft preferred so	plution				
	Plan Cisco Secure Firewall Threat Defense V Create					
Circ	Leverage Azure Traffic Manager Integrate with Azure Transit VN Tales® Threat Intelligence is interested.	r for highly scalable remote access VP et for scalable inter-VNet traffic	N	Id's largest commercial threat intelli		
Lear	n more	nuce, protecting against known and		a singest commercial aneat intern	gence como.	
*For	*Forrester Total Economic Impact of Cisco Secure Firewall, 2022. www.cisco.com/go/firewallTEI					
Mo	re products from Cisco Syste	ms, Inc. <u>See All</u>				
	M	-thethere trial	alada cisco	alada 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 🗸 🗢 🗢

从Azure门户创建VM

3. 在"基本配置"页中,为设备创建资源组,选择区域,然后为VM选择名称。

Create Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG

...

Project details		
Select the subscription to manage deplo manage all your resources.	yed resources and costs. Use resource groups like folders to org	janize 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 🕕	OK Cancel	~
Software Version 🕕		~

创建新资源组

4. 从可用选项中选择VM部署所需的版本。

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. 为主帐户设置用户名,选择密码作为身份验证类型,然后设置VM访问密码和管理密码。

\equiv Microsoft Azure		م
Home > Marketplace >		
Create Cisco Secure Fire	ewall Threat Defense Virtual – BYOL and PAY	G
Basics Cisco FTDv 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 🗸	
Resource group * ①	(New) FDM V	
	Create new	
Instance details		
Region * ①	East US 🗸	
Victori Marking group to O	film	
Virtual Machine name * 🕕		
Licensing ①	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	
Addictation type 10	SSH Public Key	
Deceword *		
Password * 0	· · · · · · · · · · · · · · · · · · ·	
Confirm password *	····· ✓	
Admin Password * 🛈	······	
Confirm Admin Password * 🕕	····· ✓	
FTDv Management * ①	FDM : Firepower Device Management	

用户名和管理员密码。

6. 对于管理类型,为本文档选择FDM。

FTDv Management * 🕕

 FMC : Firepower Management Center
 \negative

 FDM : Firepower Device Management
 \negative

 FMC : Firepower Management Center
 \negative

Enter FMC registration information * 🕕

管理设备。

7. 在思科FTDv设置选项卡中,查看完成基本配置后默认创建的VM大小、存储帐户、公共IP地址和 DNS标签。

确保虚拟网络、管理子网和其他以太网设置正确。

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 V
Public IP	address ①	(new) Create new	-pip 🗸
DNS lab	el 🛈	c35	2e65c 🗸
Attach d	iagnostic interface * 🕕	NoYes	.eastus.cloudapp.azure.com
Virtual n	etwork ①	(New) vnet01 FD Edit virtual network	M
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	ice) * None Allow selected ports 	
1 AI	II traffic from the Internet will etworking page later.	be blocked by default. You will be a	ble to change inbound port rules in the VM

思科FTDv设置。

8. 选择Allow selected Port以启用端口SSH (22)、SFTunnel (8305)和HTTPS (443),从而通过 HTTPS访问虚拟机并将设备迁移到FMC的SFTunnel端口。

Virtual network 🕕	(New) vnet01	N.	\sim
	Edit virtual network		
Management subnet * 🛈	(New) subnet1		\sim
	Edit subnet	172.18.0.0 - 17	2.18.0.255 (256 addresses)
GigabitEthernet 0/0 subnet * 🕕	(New) subnet2		\sim
	Edit subnet	172.18.1.0 - 17	2.18.1.255 (256 addresses)
GigabitEthernet 0/1 subnet * 🕕	(New) subnet3		\sim
	Edit subnet	172.18.2.0 - 17	2.18.2.255 (256 addresses)
Public inbound ports (mgmt. interface) *	NoneAllow selected ports		
Select Inbound Ports (mgmt. interface) *	3 selected SSH (22)		\checkmark
A Selected ports will be open for access Networking page later.	fi SFTunnel (8305) SFTunnel: [FMC Mana and managed device(HTTPS (443) HTTPS: [FDM Manage	to the VM. agement]: default tcp port s) communication. ement]: FDM UI accessibili	8305: management center tv.

Cisco FTDv上允许的端口

验证虚拟机的配置

9. 在审核+创建选项卡中审核配置并创建虚拟机。

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)

此时,我们可以提交VM创建。

10. 在概述选项卡中监视部署进度,此选项卡上的消息指示部署正在进行。

Home >				
cisco.cisco-firepowe Deployment	er-threat-defense-appliance-			×
₽ Search «	🔋 Delete 🚫 Cancel 🚏 Redeploy 🞍 Download 🖒 Refresh			
Overview Inputs Outputs Outputs Template	Deployment is in progress Deployment name : (isto cisco-frepower-theat-defense-appliance Subscription : Resource group : Deployment details	Start time : 6/11/2024, 11:5026 AM Correlation ID :		Microsoft Defender for Cloud Secure your apps and infrastructure Go to Microsoft Defender For Cloud >
	Resource	Type S	Status Operation details	Start learning today >
	e time time time time time time time tim	Virtual machine C	Created Operation details	Work with an expert
	Idm 85089e65	Storage account C	DK Operation details	who can help manage your assets on Azure
	o Internet Nic2	Network interface C	Created Operation details	and be your first line of support.
	Star - Sdm - Nic1	Network interface C	Created Operation details	ring an Azure expert >
	Sdm NicO	Retwork interface	Created Operation details	
	vnet01	↔ Virtual network C	DK Operation details	
	Comparison (1998) 86009e65	Storage account C	DK Operation details	
	pid-4da66463-6b9b-47e7-93d5-2cbbfa4ed70d-partnercenter	Deployment C	OK Operation details	
	C fdm pip	Public IP address C	OK Operation details	
	Subnet2-RouteTable	强 Route table 🛛 🔾	DK Operation details	
	Subnet3-RouteTable	🛃 Route table 🛛 🖸	DK Operation details	
	Contraction - Data-SecurityGroup	📢 Network security group 🛛 C	DK Operation details	
	Subnet1-RouteTable	🐴 Route table C	OK Operation details	
	C fdm	💎 Network security group 🛛 C	OK Operation details	
	Give feedback			
	At Tell us about your experience with deployment			

正在部署.

检查在Azure上部署的VM

11. 创建虚拟机后,在虚拟机部分中查找该虚拟机,找出其特性和分配的公共IP地址。

- Microsoft Amure		C Search resources se	envices, and docs (G+/)				n 🕛 a	രെഗ	0
C Home >					_			Ψ 'n	~
Virtual machines 🖈 …									×
+ Create $\lor~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~$	🔘 Manage view 🗸 💍 Refresh 🞍 Export to C	5V 📽 Open query 🕴 🕅	Assign tags 🕞 Start 🔇	" Restart 🔲 Stop 🗊 Dele	ite III Services 🗸 🤌 Mainte	enance 🗸			
Filter for any field Subscription equals all	Type equals all Resource group equals all X	Location equals all \times	† _♥ Add filter						
Showing 1 to 2 of 2 records.							No grouping	✓ III List view	~
Name 1.	Type ↑↓ Subscription ↑↓	Resource group 14	Location 14	Status †4	Operating system 14	Size ↑↓	Public IP address 1	Disks †4	
-fdm-	Virtual machine -fw-azure	_FDM_	East US	Running	Linux	Standard_D3_v2	.107	1	

虚拟机位置

12. 使用浏览器导航到设备的IP地址并开始初始配置FDM。

«	fdm Virtual machine	\$ \$ ···	×
	₽ Search «	🖋 Connect 🗸 ▷ Start 🦿 Restart 🔲 Stop 🕥 Hilbernate 🞉 Capture 🍘 Delete 🖒 Refresh 🛄 Open in mobile 👰 Feedback 🐻 CLI / PS	
	Overview	A Econstitute	ICON Manu
	Activity log	* Sostiluis	JSON VIEW
	Access control (IAM)	Resource group (mixey): ILDM Clearang system : Linux (cerunina) Cathur : Diminen Claar Claarang System : Claarang Corport of globard : Glob macroood	
	🥏 Tags	Location : East US Public IP address : 8:107 D	
	X Diagnose and solve problems	Subscription (move) : <u>ife-azure</u> . Virtual network/subnet : <u>yme01/subnet1</u>	
	Connect	Subscription ID : -ca20fa3e1482 DNS name : (dm 52e65c.eastus.cloudapp.azure.com	
	Ø Connect	Health state : -	
	× Bastion	Time created : 6/11/2024, 5:50 PM UTC	
	Networking	Tags (<u>edit</u>) : <u>Add tags</u>	

FDM的公共IP

FDM的基本配置

13. 配置基本设置,方法是选择指定范围内的IP,设置NTP,并使用许可证注册设备。

您可以在此处找到FDM初始配置的文档。

$\leftarrow \ \rightarrow \ \mathbf{G}$	O 🏝 https://	18.107/#/easysetup/step	p-1						80% 公	*
Firewall Device Manager		Device: fdm					?	admin Administrator	v elisco SECURE	
			Rade Network	Cisco Firepower Threat Defense for Asure @	NOMT CONSOLE	SP/WAV/Gase	Intern ONS S NTP Se ONS Se ONS Se ONS Se ONS Se ONS Se	not Inver		
				Connect fire The initial access control polic You can edit th Rule 1 Trust Outbound Traffic This nule allows traffic to go from inside to outside, which is needed for the Smart License configuration.	wall to Internet y will enforce the following ac e policy after setup. Default Action Block all other traffic The default action blocks all traffic.	other				
				Outside Interface Address Connect GigabitEthemet0/0 (Outside your cable modem or router. Then, co interface. Configure IPv4) to your ISP/WAN device, for enfigure the addresses for the c	xample, utside				
				IPv4 Address .1.15 Network Mask						
				255.255.0 Gateway .1.1 Configure IPv6		Ť	0			
				IPv6 Address Disabled Prefix Length		v				
FDM的基本配置				Disabled						

14. 注册设备后,确保不保留任何待处理的部署。



关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。