

Implantar VM do FDM do Azure Marketplace Usando Modelo

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Implantar FDM do Modelo no Portal do Azure](#)

[Verificar a configuração da VM](#)

[Verificar VM Implantada no Azure](#)

[Configuração Básica do FDM](#)

Introdução

Este documento descreve a implantação do Cisco Secure Firewall Threat Defense Virtual (FDM) em uma máquina virtual usando o Azure Marketplace e modelos.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Firewall Management Center (FMC)
- Defesa contra ameaças (FTD) do Cisco Secure Firewall
- Conta/Acesso do Azure

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco Secure Firewall Threat Defense Versões virtuais: 7.4.1, 7.3.1, 7.2.7, 7.1.0, 7.0.6 e 6.4.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

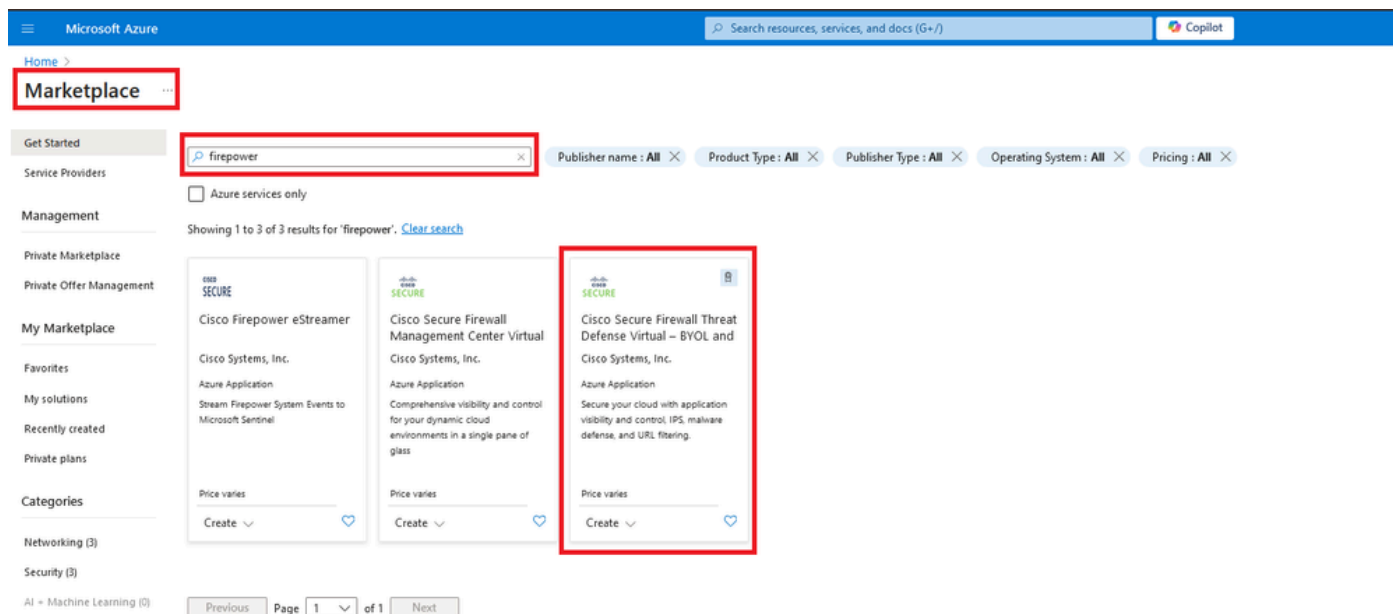
Configurar

Os clientes encontraram problemas ao tentar implantar um Firepower Device Manager (FDM) em uma máquina virtual do Azure, especificamente ao usar o Azure Marketplace e modelos.

Implantar FDM do Modelo no Portal do Azure

Para implantar o FDM no portal do Azure, use este procedimento:

1. Navegue até o portal do Azure e localize o Marketplace nos Serviços do Azure. Procure e selecione Cisco Secure Firewall Threat Defense Virtual - BYOL e PAYG.



Procure Firepower e selecione Cisco Secure Firewall Threat Defense Virtual - BOYL

2. Clique em Criar para iniciar o processo de configuração do FTD.

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</p> <p>Cisco Systems, Inc.</p> <p>Azure Application</p> <p>A Cisco Meraki Virtual MX to connect your Meraki network to your Azure deployments</p> <p>Starts at Free</p> <p>Create</p>	<p>Cisco Catalyst 8000V Edge Software (PAYG)</p> <p>Cisco Systems, Inc.</p> <p>Virtual Machine</p> <p>Deploy and manage enterprise-class networking services and VPN technologies for the Azure cloud.</p> <p>Starts at \$2.53/hour</p> <p>Create</p>	<p>Cisco Catalyst 8000V Edge Software - Solution</p> <p>Cisco Systems, Inc.</p> <p>Azure Application</p> <p>Deploy and manage enterprise-class networking services and VPN technologies for the Azure cloud.</p> <p>Price varies</p> <p>Create</p>	<p>Cisco Nexus Dashboard</p> <p>Cisco Systems, Inc.</p> <p>Azure Application</p> <p>Simplified, centralized data center dashboard makes it easier to manage your hybrid cloud network</p> <p>Price varies</p> <p>Create</p>
---	---	--	---

Criar VM do Portal do Azure

3. Na página de configuração básica, crie um Grupo de Recursos para o dispositivo, escolha a região e selecione um nome para a 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

Criar um novo Grupo de Recursos

4. Escolha a versão desejada para a implantação da VM nas opções disponíveis.

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

Versões Disponíveis para Implantação no Azure Market

5. Configure um nome de usuário para a conta Principal, escolha Senha como o tipo de Autenticação e defina a Senha para acesso à VM e a senha de Admin.

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 * ⓘ

Nome de usuário e Senhas de administrador.

6. Para o tipo de gerenciamento, selecione FDM para a finalidade deste documento.

FTDv Management * ⓘ

Enter FMC registration information * ⓘ

FMC : Firepower Management Center

FDM : Firepower Device Management

FMC : Firepower Management Center

Management Device (Dispositivo de gerenciamento).

7. Na guia Cisco FTDv Settings, revise o tamanho da VM, a conta de armazenamento, o endereço IP público e o rótulo DNS, que são criados por padrão após concluir a configuração básica.

Certifique-se de que a rede virtual, a sub-rede de gerenciamento e outras configurações de Ethernet estejam corretas.

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 Settings (Configurações de FTDv Cisco).

8. Selecione Allow seleted Port para ativar as portas SSH (22), SFTunnel (8305) e HTTPS (443) para acesso HTTPS à VM e porta SFTunnel para migração do dispositivo para o FMC.

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

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.

Portas a serem permitidas no Cisco FTDv

Verificar a configuração da VM

9. Revise a configuração na guia Revisar + Criar e crie a 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

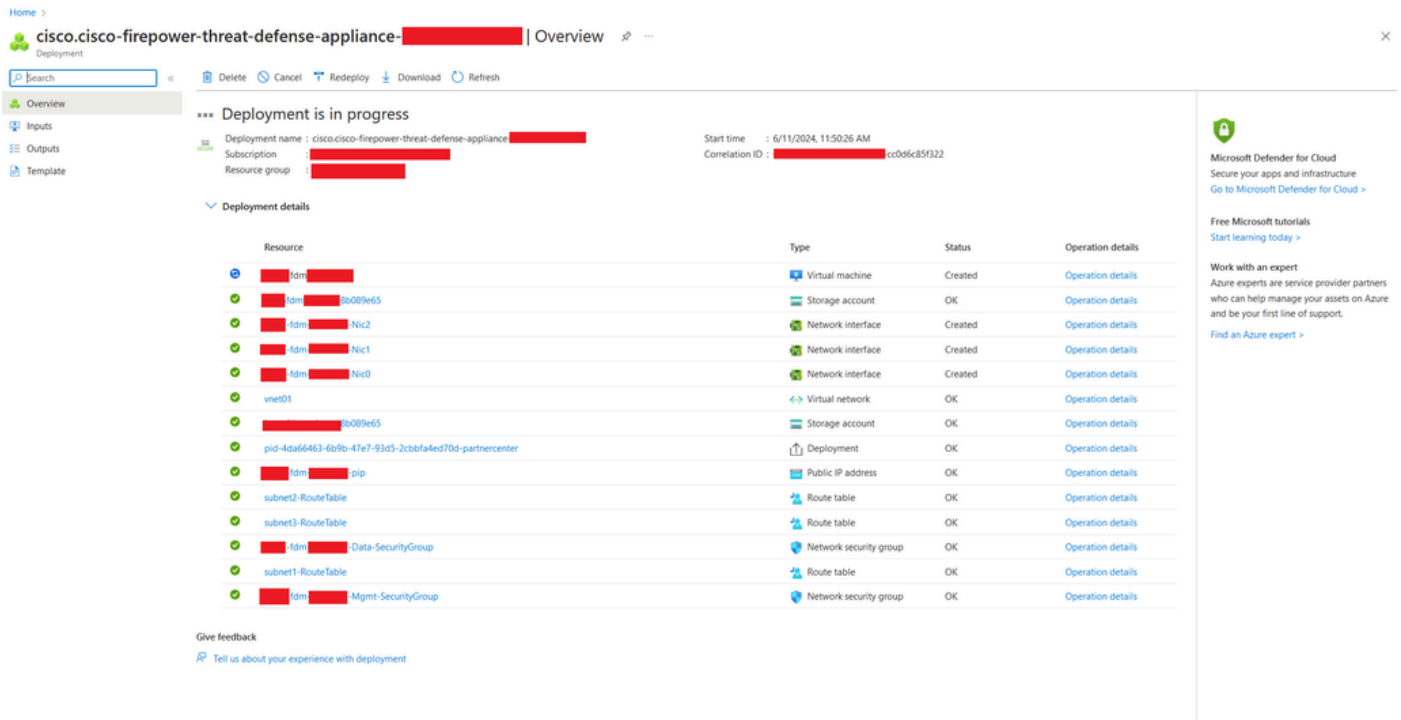
Virtual machine size	Standard_D3_v2
Storage account	<input type="text" value="8b089e65"/>
Public IP address	<input type="text" value="fdm- -pip"/>
Domain name label	<input type="text" value="-fdm- -c352e65c"/>
Attach diagnostic interface	No

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)

Revisar e criar.

Neste ponto, podemos enviar a criação da VM.

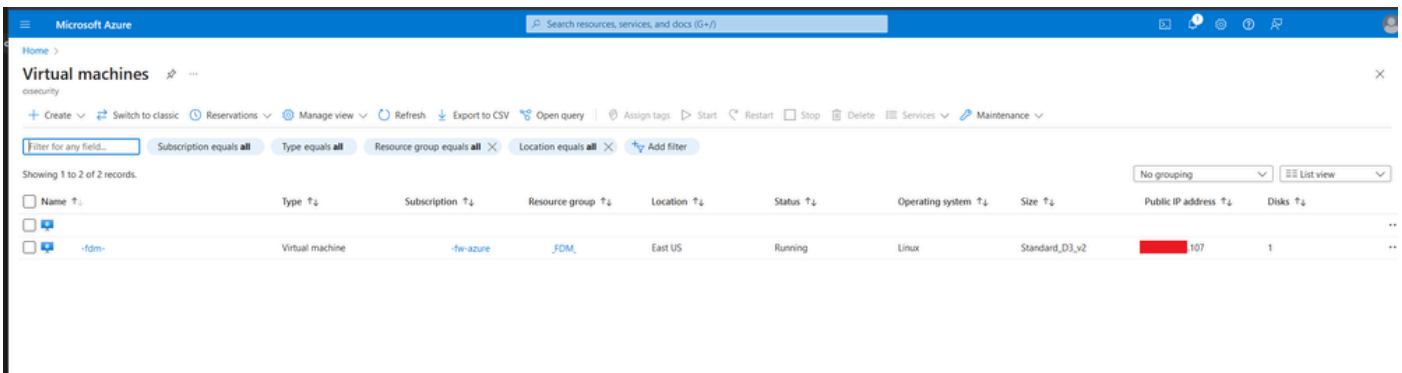
10. Monitore o andamento da disponibilização na guia Visão Geral, onde uma mensagem indica que a Disponibilização está em andamento.



Implantação em andamento.

Verificar VM Implantada no Azure

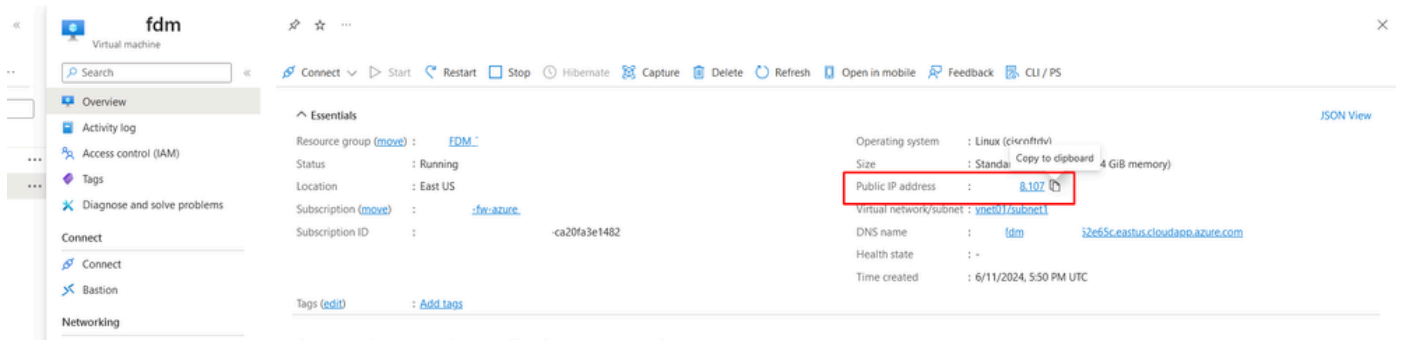
11. Quando a VM for criada, localize-a na seção Máquinas virtuais para encontrar suas características e o endereço IP público atribuído.



Localização de Máquinas Virtuais

12. Use um navegador para navegar até o endereço IP atribuído ao dispositivo e inicie a

configuração inicial do FDM.



IP Público para FDM

Configuração Básica do FDM

13. Defina as configurações básicas selecionando um IP dentro do intervalo designado, configurando o NTP e registrando o dispositivo com a licença.

Aqui você pode encontrar a documentação da [Configuração Inicial do FDM](#).

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

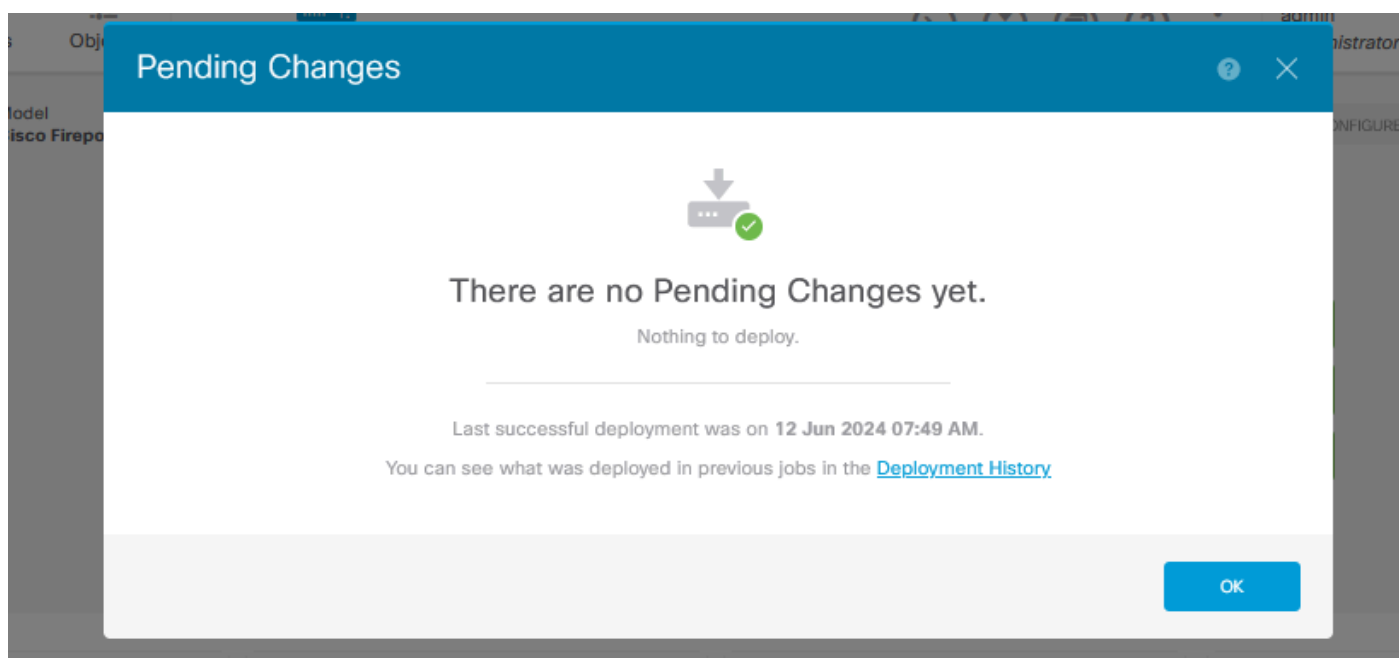
Off

IPv6 Address: Disabled

Prefix Length: Disabled

Configuração Básica no FDM

14. Após registrar o dispositivo, assegure-se de que nenhuma implantação pendente permaneça.



Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.