Distribuisci VM FDM da Azure Marketplace tramite il modello

Sommario

Introduzione

In questo documento viene descritta la distribuzione di Cisco Secure Firewall Threat Defense Virtual (FDM) in una macchina virtuale utilizzando Azure Marketplace e i modelli.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)
- Account/accesso di Azure

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Cisco Secure Firewall Threat Defense versioni virtuali: 7.4.1, 7.3.1, 7.2.7, 7.1.0, 7.0.6 e 6.4.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

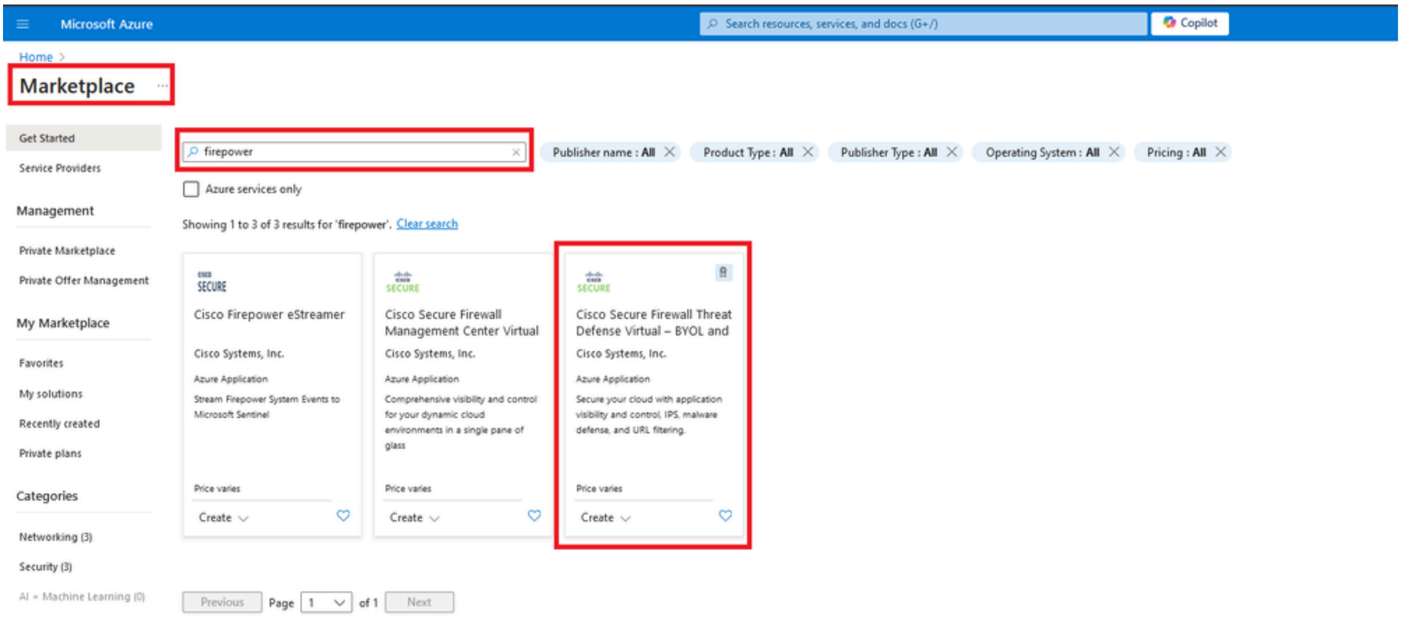
Configurazione

I clienti hanno riscontrato problemi durante il tentativo di distribuire Firepower Device Manager (FDM) in una macchina virtuale da Azure, in particolare quando si utilizzano il Marketplace di Azure e i modelli.

Distribuisci FDM dal modello nel portale di Azure

Per distribuire FDM dal portale di Azure, utilizzare la procedura seguente:

1. Passare al portale di Azure e individuare il Marketplace nei servizi di Azure. Cercare e selezionare Cisco Secure Firewall Threat Defense Virtual - BYOL e PAYG.



firepower

Showing 1 to 3 of 3 results for 'firepower'. Clear search

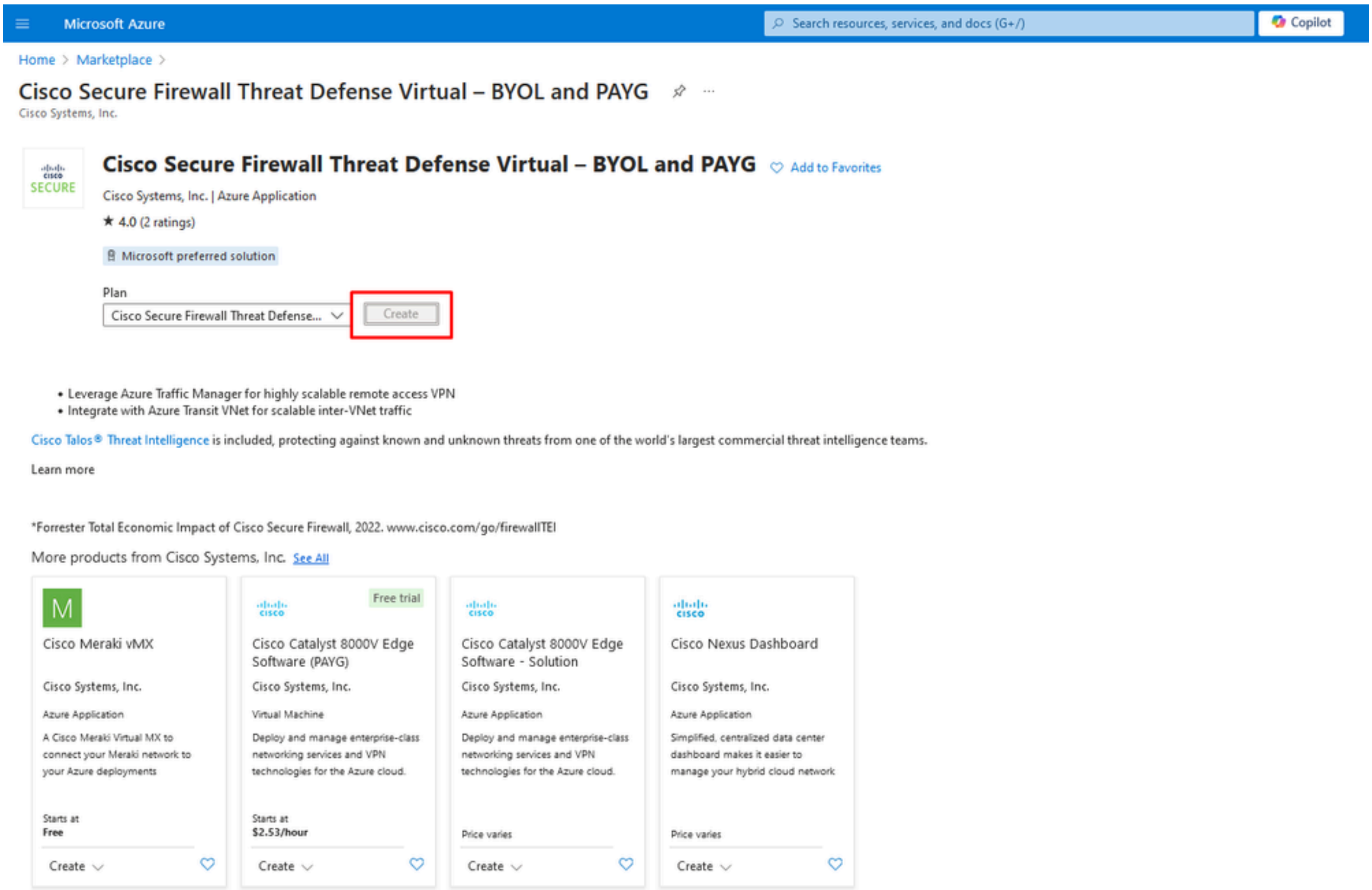
Cisco Firepower eStreamer
Cisco Systems, Inc.
Azure Application
Stream Firepower System Events to Microsoft Sentinel
Price varies

Cisco Secure Firewall Management Center Virtual
Cisco Systems, Inc.
Azure Application
Comprehensive visibility and control for your dynamic cloud environments in a single pane of glass
Price varies

Cisco Secure Firewall Threat Defense Virtual – BYOL and
Cisco Systems, Inc.
Azure Application
Secure your cloud with application visibility and control, IPS, malware defense, and URL filtering.
Price varies

Cerca Firepower e seleziona Cisco Secure Firewall Threat Defense Virtual - BOYL

2. Fare clic su Crea per avviare il processo di configurazione per l'FTD.



Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG

Cisco Systems, Inc.

Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG

Cisco Systems, Inc. | Azure Application

★ 4.0 (2 ratings)

Microsoft preferred solution

Plan: Cisco Secure Firewall Threat Defense...

- 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.

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

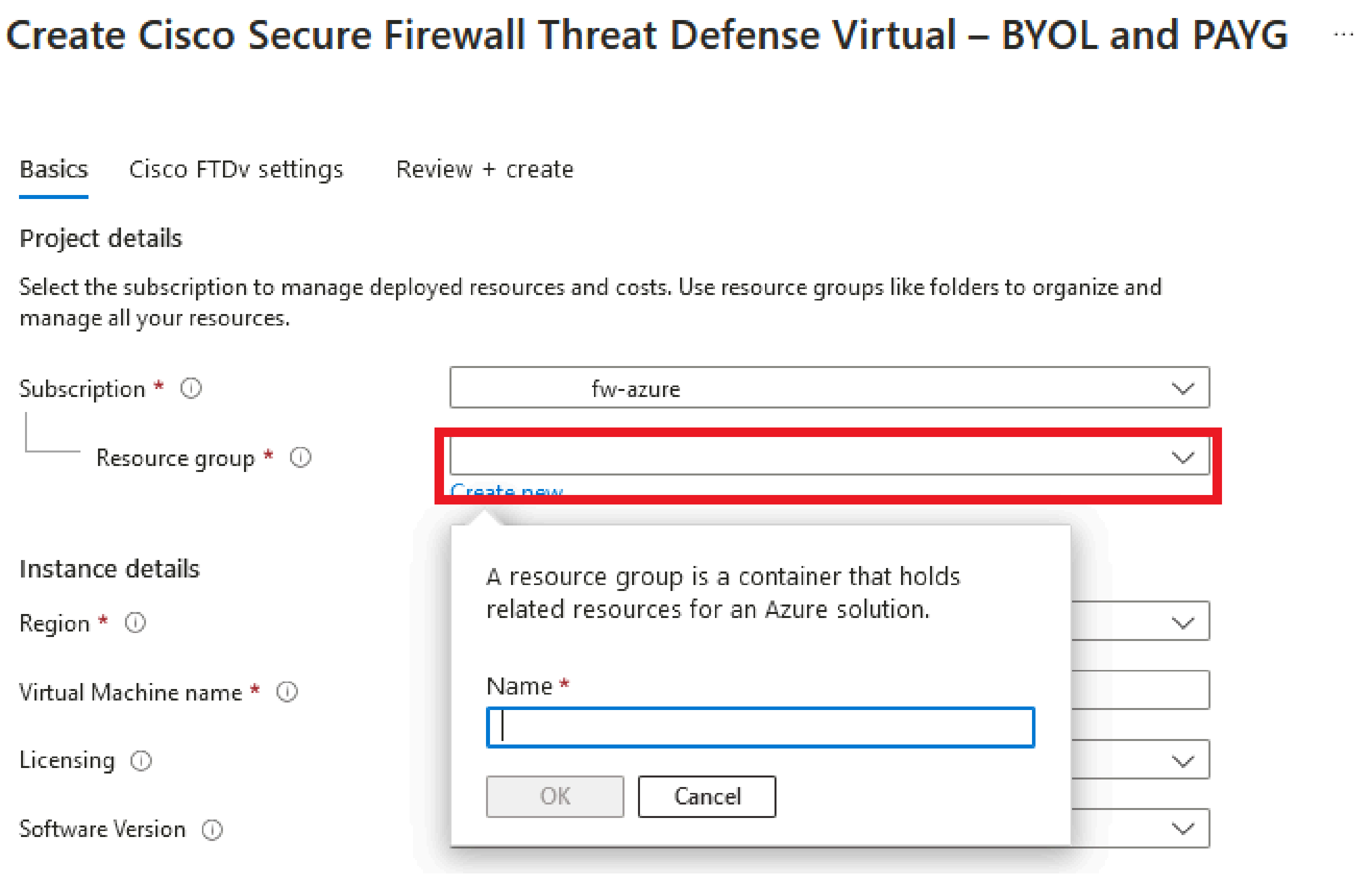
Cisco Catalyst 8000V Edge Software (PAYG)
Cisco Systems, Inc.
Virtual Machine
Deploy and manage enterprise-class networking services and VPN technologies for the Azure cloud.
Starts at $2.53/hour

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

Cisco Nexus Dashboard
Cisco Systems, Inc.
Azure Application
Simplified, centralized data center dashboard makes it easier to manage your hybrid cloud network
Price varies

Crea macchina virtuale dal portale di Azure

3. Nella pagina di configurazione di base, creare un gruppo di risorse per il dispositivo, scegliere l'area e selezionare un nome per la macchina virtuale.



Create Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG

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

Resource group * :

Instance details

Region *

Virtual Machine name *

Licensing

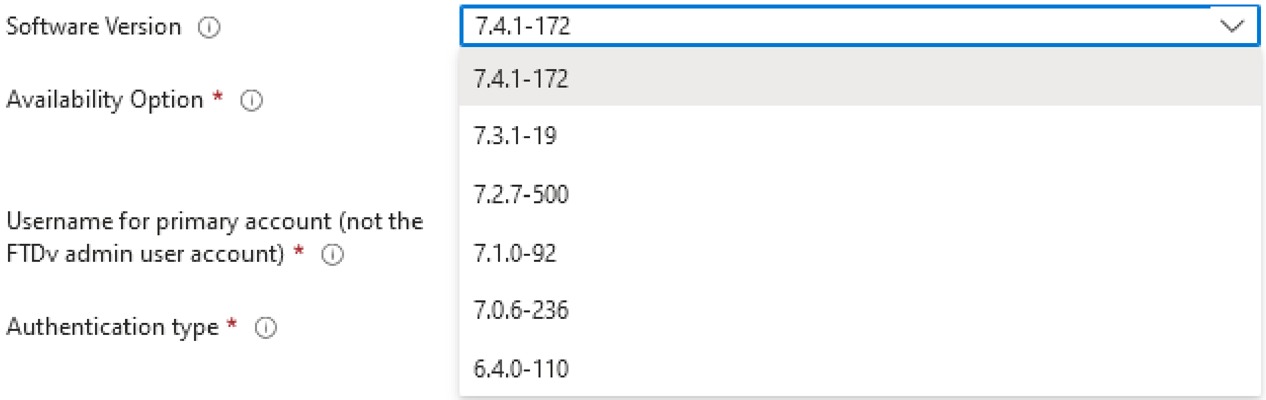
Software Version

A resource group is a container that holds related resources for an Azure solution.

Name * :

Crea un nuovo gruppo di risorse

4. Scegliere la versione desiderata per la distribuzione della VM tra le opzioni disponibili.



Software Version: 7.4.1-172

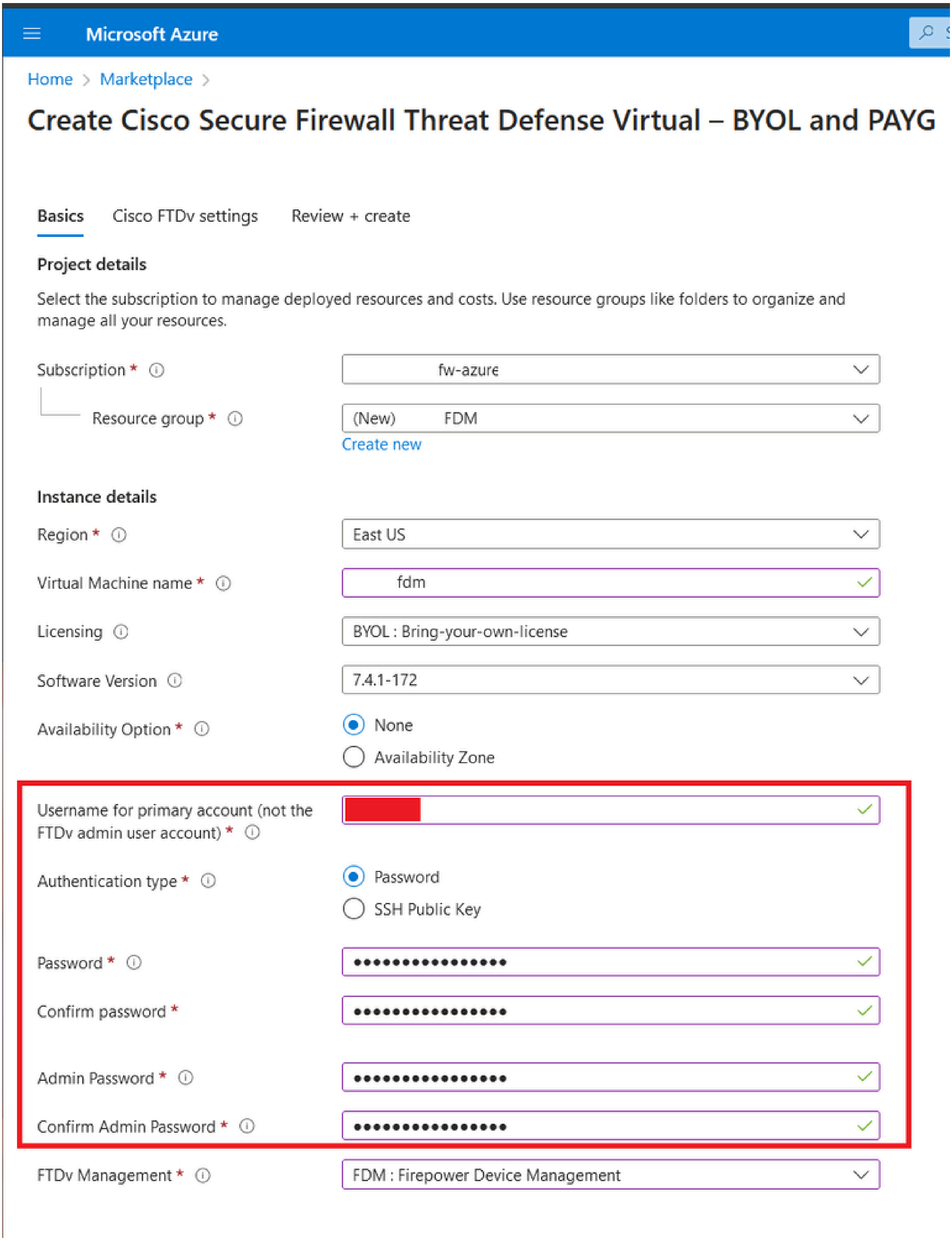
Availability Option *

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

Authentication type *

Versioni disponibili per la distribuzione nel mercato di Azure

5. Impostare un nome utente per l'account principale, scegliere Password come tipo di autenticazione e impostare la password per l'accesso alla macchina virtuale e la password amministratore.



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.

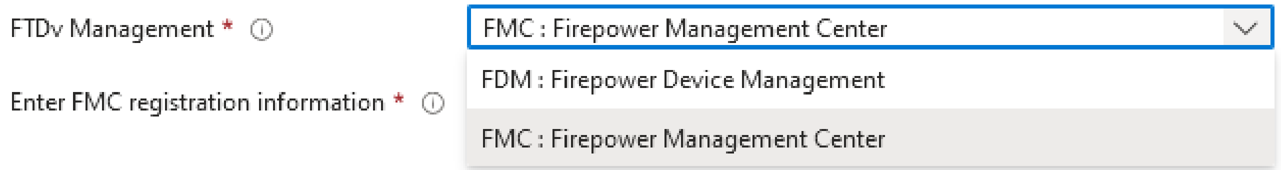
Subscription * ⓘ	fw-azure
Resource group * ⓘ	(New) FDM Create new

Instance details

Region * ⓘ	East US
Virtual Machine name * ⓘ	fdm ✓
Licensing ⓘ	BYOL : Bring-your-own-license
Software Version ⓘ	7.4.1-172
Availability Option * ⓘ	● None ○ Availability Zone
Username for primary account (not the FTDv admin user account) * ⓘ	[redacted] ✓
Authentication type * ⓘ	● Password ○ SSH Public Key
Password * ⓘ	•••••••••••••••• ✓
Confirm password *	•••••••••••••••• ✓
Admin Password * ⓘ	•••••••••••••••• ✓
Confirm Admin Password * ⓘ	•••••••••••••••• ✓
FTDv Management * ⓘ	FDM : Firepower Device Management

Nome utente e password amministratore.

6. Per il tipo di gestione, selezionare FDM ai fini del presente documento.



FTDv Management * FMC : Firepower Management Center

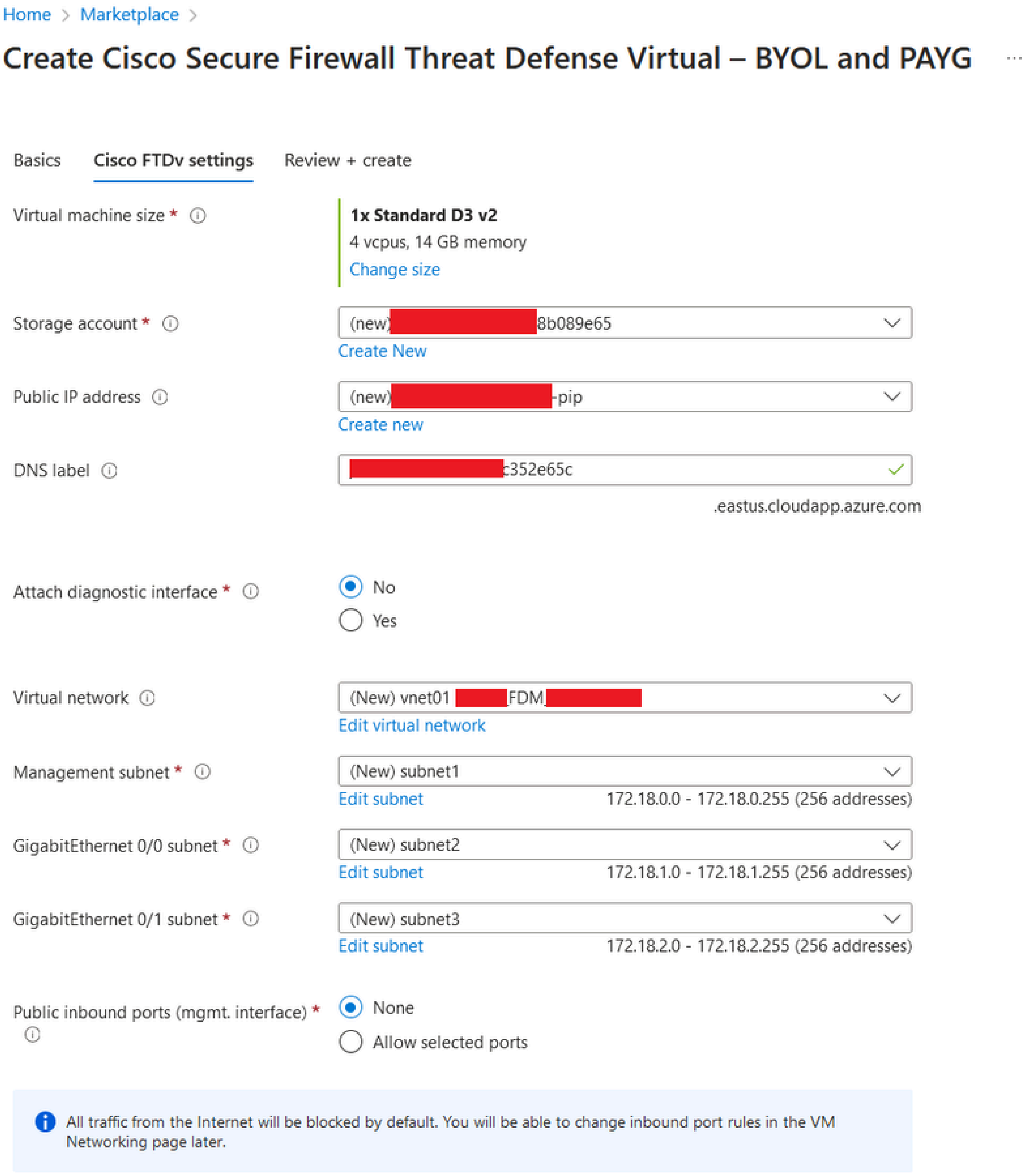
Enter FMC registration information *

FDM : Firepower Device Management
FMC : Firepower Management Center

Dispositivo di gestione.

7. Nella scheda Cisco FTDv Settings, esaminare le dimensioni della macchina virtuale, l'account di archiviazione, l'indirizzo IP pubblico e l'etichetta DNS, che vengono create per impostazione predefinita dopo il completamento della configurazione di base.

Verificare che la rete virtuale, la subnet di gestione e altre impostazioni Ethernet siano corrette.



Home > Marketplace >

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]c352e65c ✓
.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)

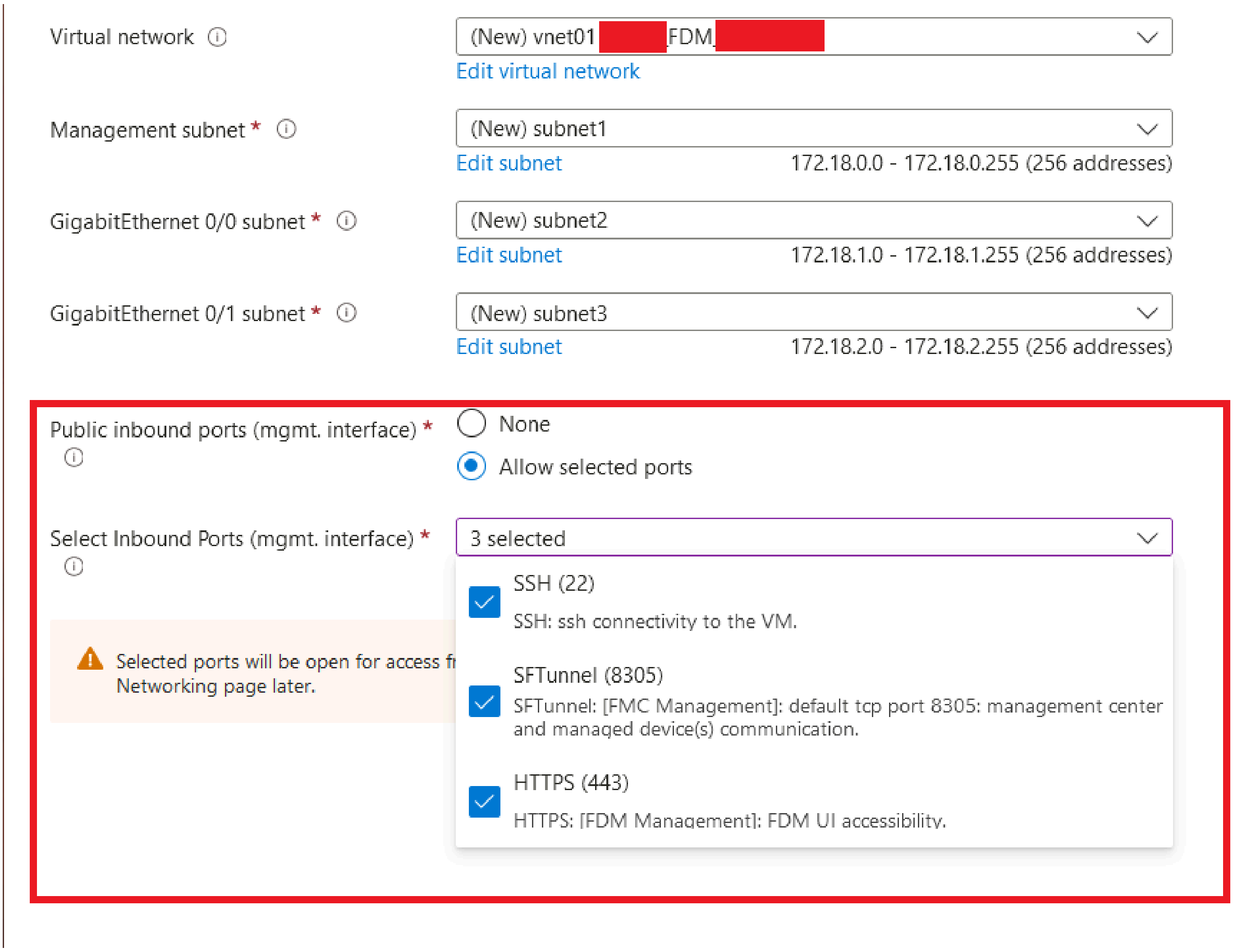
GigabitEthernet 0/1 subnet * ⓘ: (New) subnet3
Edit subnet 172.18.2.0 - 172.18.2.255 (256 addresses)

Public inbound ports (mgmt. interface) * ⓘ: ● None ○ Allow selected ports

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.

Impostazioni Cisco FTDv.

8. Selezionare Allow selected Port (Consenti porta selezionata) per abilitare le porte SSH (22), SFTunnel (8305) e HTTPS (443) per l'accesso HTTPS alla porta VM e SFTunnel per la migrazione del dispositivo a 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.

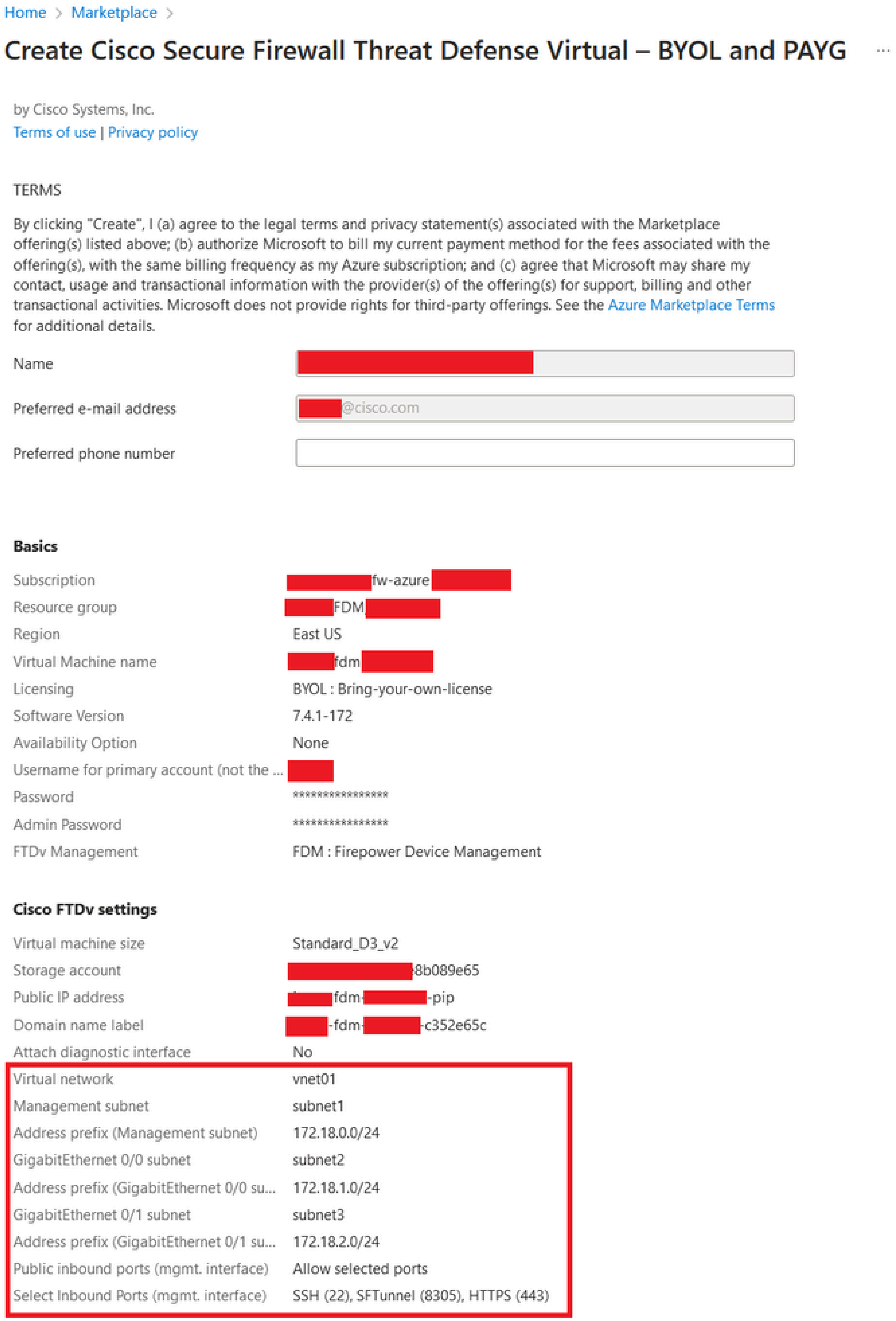
☑ HTTPS (443)
HTTPS: [FDM Management]: FDM UI accessibility.

⚠ Selected ports will be open for access fr
Networking page later.

Porte consentite su Cisco FTDv

Verifica configurazione per macchina virtuale

9. Esaminare la configurazione nella scheda Revisione + Creazione e creare la VM.



Home > Marketplace >

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	[redacted]
Preferred e-mail address	[redacted]@cisco.com
Preferred phone number	

Basics

Subscription	[redacted]fw-azure[redacted]
Resource group	[redacted]FDM[redacted]
Region	East US
Virtual Machine name	[redacted]fdm[redacted]
Licensing	BYOL : Bring-your-own-license
Software Version	7.4.1-172
Availability Option	None
Username for primary account (not the ...	[redacted]
Password	****************
Admin Password	****************
FTDv Management	FDM : Firepower Device Management

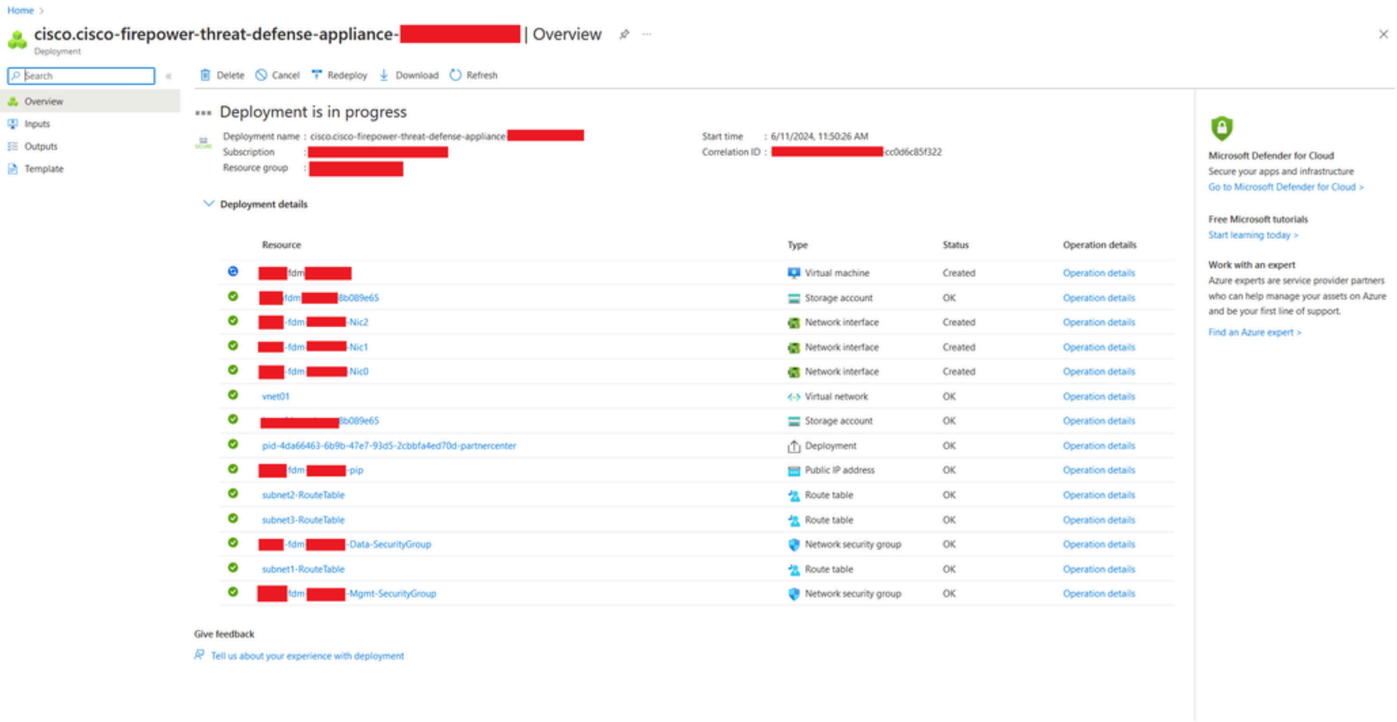
Cisco FTDv settings

Virtual machine size	Standard_D3_v2
Storage account	[redacted]8b089e65
Public IP address	[redacted]fdm-[redacted]-pip
Domain name label	[redacted]-fdm-[redacted]-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)

Revisione e creazione.

A questo punto è possibile inviare la creazione della VM.

10. Controllare lo stato della distribuzione nella scheda Panoramica, dove un messaggio indica che la distribuzione è in corso.



cisco.cisco-firepower-threat-defense-appliance-[redacted] | Overview

Deployment is in progress

Deployment name : cisco.cisco-firepower-threat-defense-appliance[redacted]
Subscription : [redacted]
Resource group : [redacted]

Start time : 6/11/2024, 11:50:26 AM
Correlation ID : [redacted]cc0d6c85f322

Deployment details

Resource	Type	Status	Operation details
[redacted]fdm[redacted]	Virtual machine	Created	Operation details
[redacted]fdm[redacted]8b089e65	Storage account	OK	Operation details
[redacted]-fdm-[redacted]-Nic2	Network interface	Created	Operation details
[redacted]-fdm-[redacted]-Nic1	Network interface	Created	Operation details
[redacted]-fdm-[redacted]-Nic0	Network interface	Created	Operation details
vnet01	Virtual network	OK	Operation details
[redacted]8b089e65	Storage account	OK	Operation details
pid-4da66463-6b9b-47e7-93d5-2cbbfa4ed70d-partnercenter	Deployment	OK	Operation details
[redacted]fdm-[redacted]-pip	Public IP address	OK	Operation details
subnet2-RouteTable	Route table	OK	Operation details
subnet3-RouteTable	Route table	OK	Operation details
[redacted]-fdm-[redacted]-Data-SecurityGroup	Network security group	OK	Operation details
subnet1-RouteTable	Route table	OK	Operation details
[redacted]fdm-[redacted]-Mgmt-SecurityGroup	Network security group	OK	Operation details

Give feedback

Tell us about your experience with deployment

Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >

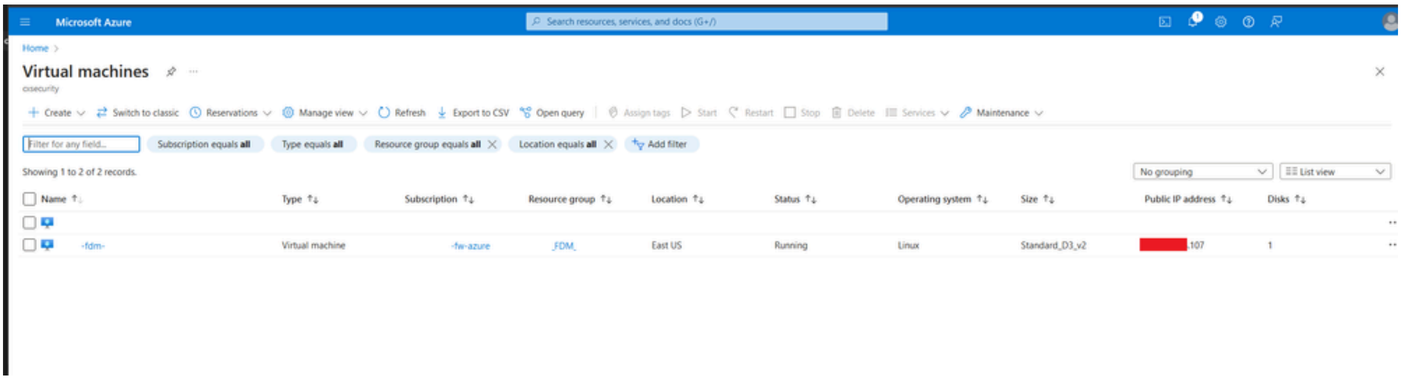
Free Microsoft tutorials
Start learning today >

Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
Find an Azure expert >

Implementazione in corso.

Verifica la macchina virtuale distribuita in Azure

11. Al momento della creazione della macchina virtuale, individuarla nella sezione Macchine virtuali per individuare le caratteristiche e l'indirizzo IP pubblico assegnato.



Virtual machines

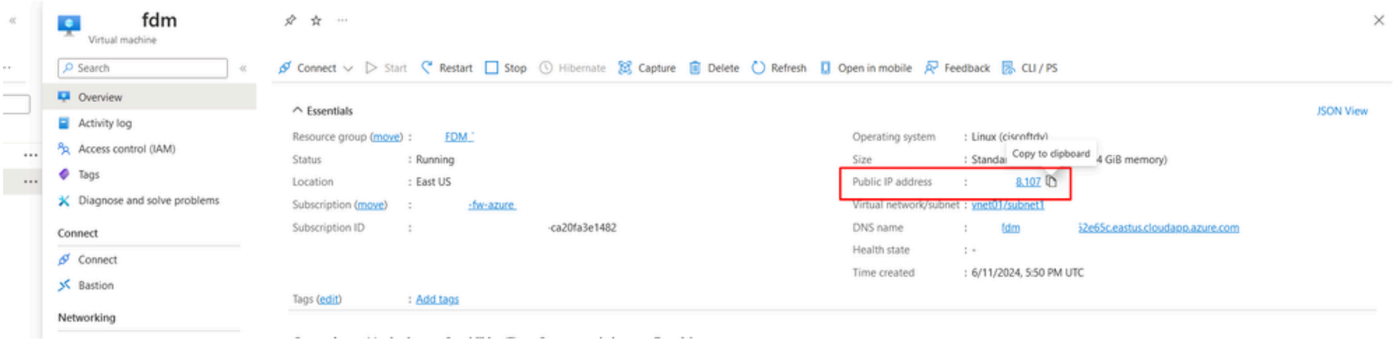
Showing 1 to 2 of 2 records.

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

Percorso macchine virtuali

12. Utilizzare un browser per passare all'indirizzo IP assegnato del dispositivo e iniziare la

configurazione iniziale di FDM.



fdm
Virtual machine

Connect | Start | Restart | Stop | Hibernate | Capture | Delete | Refresh | Open in mobile | Feedback | CLI / PS

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Connect
Bastion
Networking

Essentials

JSON View

Resource group (move) : FDM
Status : Running
Location : East US
Subscription (move) : -fw-azure
Subscription ID : -ca20fa3e1482
Tags (edit) : Add tags

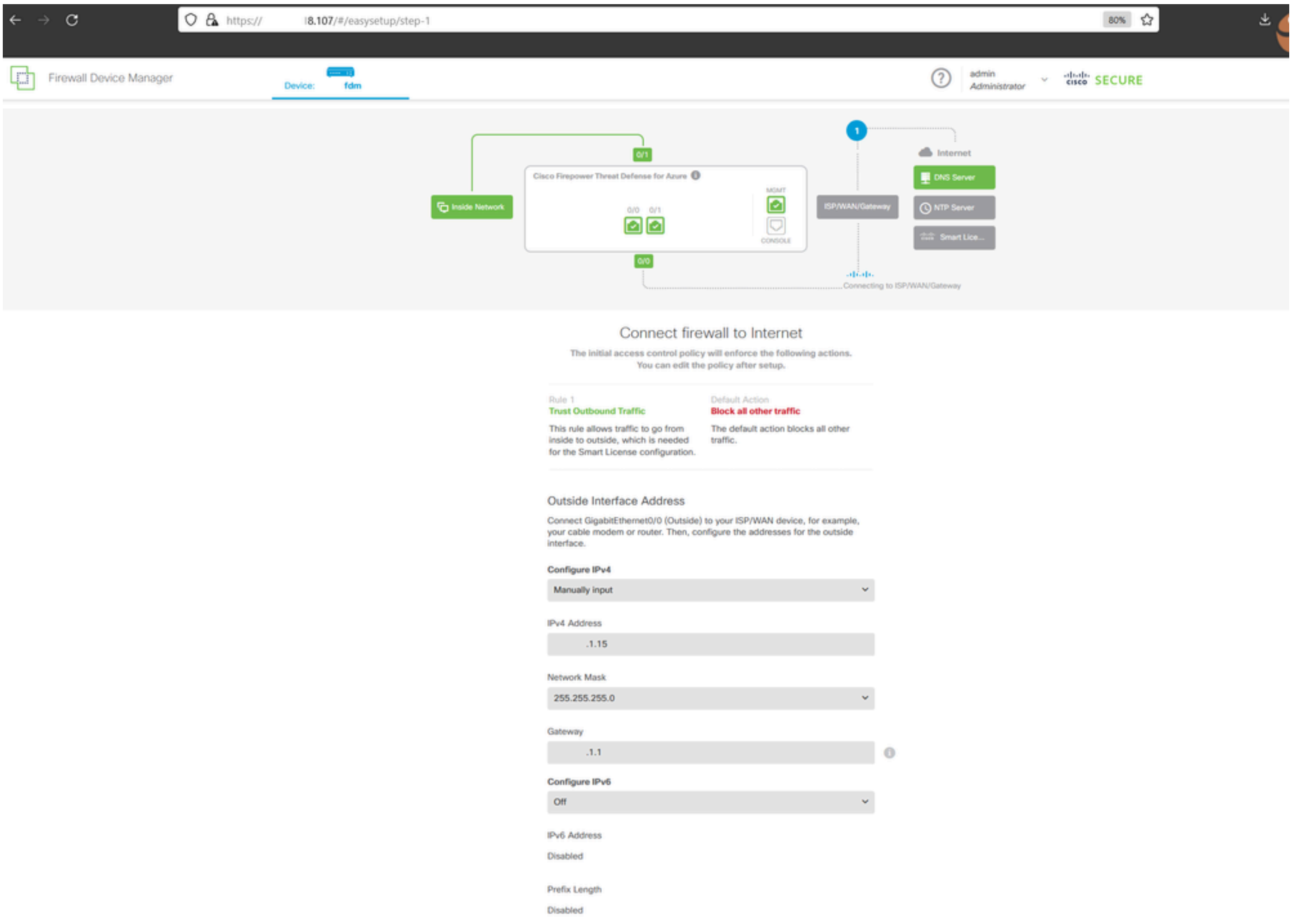
Operating system : Linux (ciscoftdv)
Size : Standa[Copy to clipboard] 4 GiB memory)
Public IP address : 8.107
Virtual network/subnet : vnet01/subnet1
DNS name : fdm 52e65c.eastus.cloudapp.azure.com
Health state : -
Time created : 6/11/2024, 5:50 PM UTC

IP pubblico per FDM

Configurazione di base per FDM

13. Configurare le impostazioni di base selezionando un indirizzo IP nell'intervallo assegnato, configurando l'NTP e registrando il dispositivo con la licenza.

In questa sezione è disponibile la documentazione relativa alla configurazione iniziale di FDM.



https:// 8.107/#/easysetup/step-1

Connect firewall to Internet

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

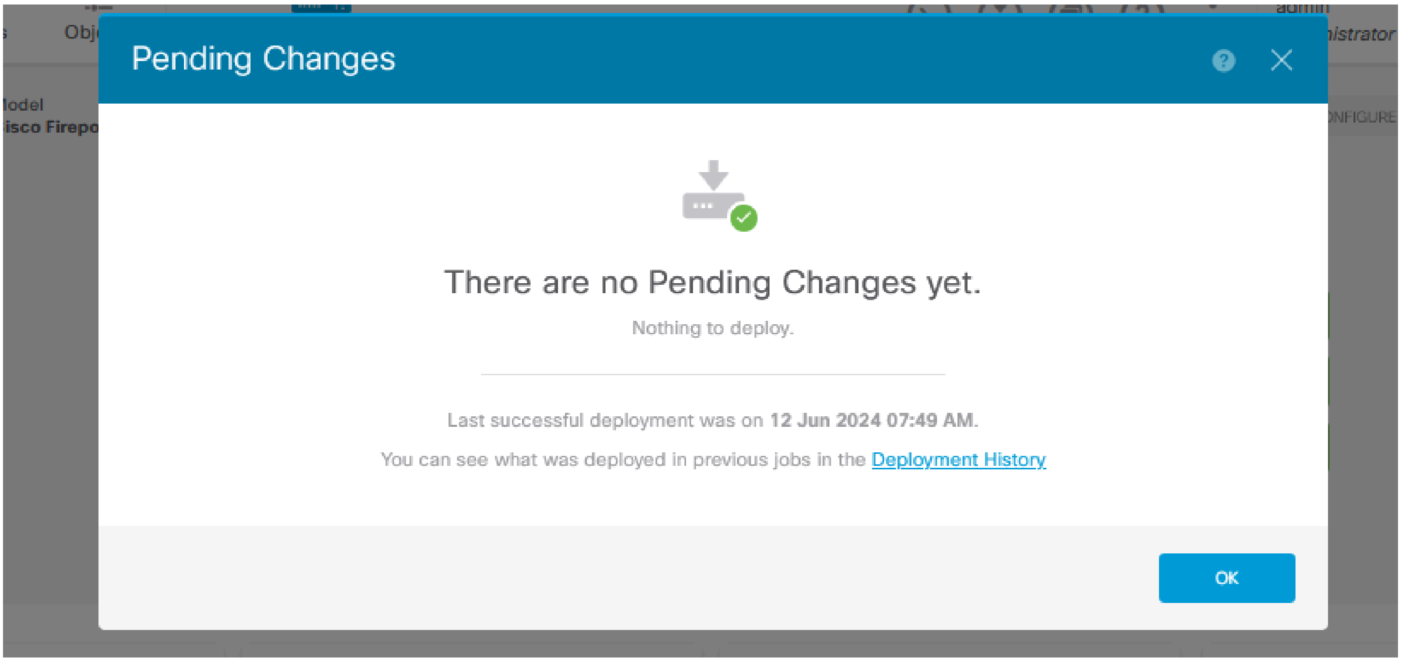
Configure IPv6: Off

IPv6 Address: Disabled

Prefix Length: Disabled

Configurazione di base in FDM

14. Dopo aver registrato il dispositivo, assicurarsi che non rimangano distribuzioni in sospeso.



Pending Changes

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